网管天下

刘晓辉 编著

交换机·路由器·防火墙

JIAOHUANJI LUYOUQI FANGHUOQIANG

（第3版）

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

VISIT…

LANZAROTE Caliente.com

内 容 简 介

本书深入细致地介绍了用于构建网络的最重要的硬件设备——交换机、路由器和防火墙，涵盖了原理、参数、分类、适用、规划、接口、连接、配置、管理、监控、故障等诸多方面，体现并融合了最新技术、最新设备和最新应用，是一整套紧贴网络搭建、配置和管理实际的完全硬件解决方案。本书突出实用性和可操作性，语言表述流畅准确，理论讲解深入浅出，具体操作详略得当，注重培养动手能力和分析能力。

本书适用于中小型网络管理员，以及所有准备从事网络管理的网络爱好者，并可作为大专院校计算机专业的教材。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

交换机·路由器·防火墙 / 刘晓辉编著．—3 版．—北京：电子工业出版社，2015.1
（网管天下）
ISBN 978-7-121-25204-4

Ⅰ．①交… Ⅱ．①刘… Ⅲ. ①计算机网络－信息交换机②计算机网络－路由选择③计算机网络－安全技术Ⅳ. ①TN915.05②TP393.08

中国版本图书馆 CIP 数据核字（2014）第 299605 号

策划编辑：祁玉芹
责任编辑：鄂卫华
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：35　字数：896 千字
版　　次：2007 年 8 月第 1 版
　　　　　2015 年 1 月第 3 版
印　　次：2015 年 1 月第 1 次印刷
定　　价：69.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

交换机、路由器和防火墙构成网络硬件的金三角。交换机实现计算机互联，构建局域网络；路由器实现网络互联，构建广域网络；防火墙实现互联限制，构建安全网络。没有交换机计算机之间就无法通信，就不能搭建局域网络，因此，交换机是网络构建的基石。没有路由器就不能实现与其他网络和 Internet 的连接，局域网就会成为信息孤岛，所以，路由器是网络互联的桥梁。没有防火墙就不能实现网络内部的安全，客户端、服务器和数据信息就没有宁日，故而，防火墙是安全稳定的保障。可见，交换机、路由器和防火墙三者各司其职、相互结合、缺一不可。

与其他网络类图书不同，本书从一个全新的角度，深入、全面、细致地介绍了交换机、路由器和防火墙的原理、参数、分类、适用、规划、接口、连接、配置、管理、监控、故障等诸多方面的内容，涵盖了从规划设计、网络搭建、设备配置，到状态监控、故障诊断的所有重要硬件技术，是一本专门为大中型网络管理员定身打造的硬件设备教程，以迅速完成从电脑爱好者向专业网管员的过渡。

本书作为畅销图书《交换机·路由器·防火墙》的第 3 版，在第 2 版的基础上进行了全面修订，不仅调整了部分结构，更新了许多理论和技术，而且还介绍了一些最新的硬件网络设备，以全力突出其先进性和实用性。

全书共分为 18 章。第 1 章网络设备综述，分别介绍了交换机、路由器和防火墙在网络中的作用和应用。第 2 章至第 7 章，介绍了交换技术、交换机的分类与适用、参数与选择、端口与连接、状态与检测，以及交换机的配置与管理。第 8 章至第 13 章，介绍了路由协议、路由器的分类与适用、参数与选择、端口与连接、状态与检测，以及路由器的配置与管理。第 14 章至第 18 章，介绍了安全设备的工作原理，IPS、IDS 和防火墙的优势与适用、参数与选择、端口与连接、状态与检测，以及安全设备的配置和管理。

本书主要由刘晓辉编著，参加编写的还有肖铁岭、李海宁、田俊乐、陈志成、王春海、王淑江、赵卫东、刘淑梅、杨伏龙、李文俊、王同明、石长征、莫展宏、白华、刘媛、郭腾、马

倩等。笔者长期从事网络建设、网络管理、网络教学和网络实验工作，具有较高的理论水平和丰富的实践经验，曾经出版过 50 余部网络和系统方向的图书，均以易读、易学、实用的特点，得到众多读者的一致好评，并取得了不错的销售业绩。本书是笔者的又一呕心沥血之作，希望能对大家搭建和管理网络有所帮助。

编　者

2014 年 11 月

目录

CONTENTS

第 1 章　交换机·路由器·防火墙综述 1

1.1　交换机概述.. 1
1.1.1　交换机的功能............................. 1
1.1.2　交换机与交换式网络................. 2
1.1.3　交换机的工作原理..................... 3
1.2　路由器概述.. 5
1.2.1　路由器的功能............................. 5
1.2.2　路由器的工作原理..................... 8
1.3　防火墙概述.. 9
1.3.1　网络防火墙的功能..................... 9
1.3.2　防火墙的工作原理................... 12
1.4　网络设备在网络中的应用.............. 13
1.4.1　交换机在网络中的应用........... 13
1.4.2　路由器在网络中的应用........... 15
1.4.3　防火墙在网络中的应用........... 17

第 2 章　交换技术 19

2.1　高速以太网技术.............................. 19
2.1.1　1 Gibt/s 以太网技术 19
2.1.2　10 Gbit/s 以太网技术 21
2.1.3　40/100 Gbit/s 以太网技术 24
2.2　虚拟网技术...................................... 26
2.2.1　虚拟网的意义和作用............... 26
2.2.2　虚拟网的类型与适用............... 27
2.2.3　VTP 技术 30
2.2.4　私有虚拟网技术....................... 33
2.3　多层交换技术 34
2.3.1　第三层交换技术 34
2.3.2　第四层交换技术 36
2.4　链路冗余技术 37
2.4.1　扩展树技术 37
2.4.2　链路汇聚技术 44
2.4.3　路由冗余 46
2.5　VoIP 技术...50
2.5.1　IP 语音技术...............................50
2.5.2　服务质量技术 51
2.6　安全技术 52
2.6.1　基于端口的传输控制 52
2.6.2　Cisco IOS 防火墙......................53
2.6.3　IEEE 802.1x 认证......................54

第 3 章　交换机的选择与适用 57

3.1　交换机的分类与适用 57
3.1.1　智能与傻瓜交换机 57
3.1.2　固定端口与模块化交换机 58
3.1.3　接入层、汇聚层与核心层交换机 60
3.1.4　二、三、四层交换机 62
3.2　交换机的主要参数 63
3.2.1　三层交换机的主要参数 64
3.2.2　二层交换机的主要参数 68
3.3　交换机的选择策略 72
3.3.1　可网管交换机的选择 72
3.3.2　不同位置交换机的选择 75

第 4 章　交换机的端口与连接........81

4.1　IEEE 802.3 系列标准......................81
4.1.1　10 Mbps 以太网标准................81
4.1.2　100 Mbps 快速以太网标准......81
4.1.3　1 Gbps 以太网标准..................82
4.1.4　10 Gbps 以太网标准................84
4.1.5　40/100 Gbps 以太网标准.........87
4.2　交换机端口类型..............................88
4.2.1　光纤端口...................................89
4.2.2　双绞线端口...............................90
4.2.3　1GE 模块与插槽......................91
4.2.4　10GE 模块与插槽....................93
4.2.5　40GE 模块与插槽....................95
4.2.6　复用端口...................................96
4.2.7　10GE 转换模块........................97
4.3　跳线与使用......................................98
4.3.1　双绞线跳线...............................98
4.3.2　光纤跳线.................................100
4.3.3　光纤跳线与光纤端口............102
4.4　交换机的连接策略........................102
4.4.1　不同性能交换机的连接策略.102
4.4.2　非对称交换机的连接策略.....103
4.4.3　对称交换机的连接策略.........104
4.5　交换机的连接................................105
4.5.1　光纤端口的连接....................105
4.5.2　双绞线端口的连接................107
4.6　交换机的堆叠................................108
4.6.1　堆叠概述...............................108
4.6.2　StackWise 堆叠技术..............109
4.6.3　StackWise Plus 堆叠技术.......112
4.6.4　FlexStack 堆叠技术................113

第 5 章　交换机的配置方式与初始化........................117

5.1　交换机配置前的准备....................117
5.1.1　交换机配置前的规划............117
5.1.2　交换机的管理方式................118
5.1.3　交换机的配置方式................127
5.1.4　配置信息准备........................131
5.2　CLI 命令行....................................131
5.2.1　CLI 命令行及使用..................131
5.2.2　指定端口、VLAN、MAC 和 IP..138
5.3　交换机初始化配置........................140
5.3.1　图形界面初始化配置............140
5.3.2　对话式初始配置....................143
5.3.3　CLI 命令初始化配置.............145

第 6 章　使用 CLI 配置交换机......149

6.1　交换机配置前的规划....................149
6.2　配置 VLAN....................................150
6.2.1　VTP 版本和配置策略............150
6.2.2　配置 VTP................................153
6.2.3　创建和管理 VLAN.................154
6.2.4　配置中继................................159
6.3　配置链路冗余...............................164
6.3.1　配置 PVST.............................164
6.3.2　配置 MSTP.............................166
6.3.3　配置链路汇聚........................169
6.4　配置路由.......................................175
6.4.1　配置 SVI 接口........................175
6.4.2　配置物理三层接口................176
6.4.3　配置 EtherChannel 三层接口.177
6.4.4　配置三层子接口....................178
6.4.5　配置单播路由........................180
6.4.6　配置缺省网关和默认路由.....184
6.4.7　配置动态路由........................185
6.5　配置端口.......................................186
6.5.1　配置二层接口........................186
6.5.2　配置 PortFast.........................191
6.5.3　配置 UplinkFast.....................193
6.6　基于端口的传输控制....................196

6.6.1 风暴控制..196
6.6.2 端口流控制....................................198
6.6.3 端口带宽限制................................198
6.6.4 保护端口..200
6.6.5 端口阻塞..200
6.6.6 端口安全..201
6.7 配置 ACL..203
6.7.1 访问列表概述................................203
6.7.2 创建并应用 IP 访问列表 205
6.7.3 创建并应用 MAC 访问列表..211
6.7.4 创建并应用 VLAN 映射........213
6.8 其他重要配置..215
6.8.1 配置 DHCP 中继 215
6.8.2 配置 HSRP..............................218
6.8.3 配置 802.1x 基于端口的认证.......................................221

第 7 章 使用 CLI 管理和监控交换机 227

7.1 监控交换机..227
7.1.1 监控交换机系统状态.............227
7.1.2 监控端口模块和状态.............229
7.1.3 查看 MAC 地址表.................236
7.1.4 TDR 线缆测试........................236
7.2 管理交换机..236
7.2.1 TFTP 服务器 236
7.2.2 系统文件管理........................237
7.2.3 配置文件管理........................239
7.2.4 IOS 软件映像管理 243
7.3 配置网络远程管理................................247
7.3.1 配置 CDP 247
7.3.2 配置 SNMP 250
7.3.3 配置 RMON...........................253
7.3.4 配置 SPAN 和 RSPAN 257

第 8 章 路由协议 267

8.1 静态路由与默认路由............................267
8.1.1 直连路由 267
8.1.2 静态路由 268
8.1.3 默认路由 269
8.2 动态路由协议 270
8.2.1 RIP 路由协议..........................270
8.2.2 OSPF 路由协议......................272
8.2.3 EIGRP 路由协议....................276
8.2.4 IS-IS 路由协议........................278
8.2.5 BGP 路由协议 280

第 9 章 路由器的选择与适用 283

9.1 路由器的分类 283
9.1.1 按性能划分 283
9.1.2 按结构划分 285
9.1.3 按网络位置划分 285
9.1.4 按功能划分 286
9.1.5 按转发性能划分 286
9.1.6 按网络类型划分 286
9.2 路由器的参数 287
9.2.1 路由器基本参数 287
9.2.2 路由器性能参数 291
9.3 路由器的选择策略 292
9.3.1 路由器的选购原则 292
9.3.2 选购时应考虑的因素 294

第 10 章 路由器的接口与连接 295

10.1 路由器模块和接口卡 295
10.1.1 SPE 295
10.1.2 SM/SM-X 295
10.1.3 WIC/HWIC/EHWIC 296
10.1.4 PVDM/PVDM2/PVDM3/PVDM4s.................................297
10.1.5 AIM/ISM 298
10.1.6 NM/NME...............................299
10.1.7 VIC/VWIC/EVM 300
10.2 路由器接口 301

10.2.1 10Base-T/100Base-TX/1000Base-T 接口 301
10.2.2 GBIC/SFP 插槽 302
10.2.3 SC/LC 接口 303
10.2.4 T1/E1 接口........................... 303
10.2.5 智能串行接口....................... 304
10.2.6 异步/同步串口...................... 304
10.2.7 ADSL 接口 305
10.2.8 BNC 接口............................. 305
10.3 路由器的连接.............................. 306
10.3.1 路由器连接策略................... 306
10.3.2 与局域网设备的连接.......... 307
10.3.3 连接器与电缆....................... 307
10.3.4 与广域网接入设备的连接... 310
10.4 路由器的连接测试...................... 311
10.4.1 Show 命令判断..................... 311
10.4.2 LED 指示灯判断.................. 312

第 11 章 路由器的配置方式与初始化 315

11.1 路由器配置前的规划................. 315
11.2 路由器配置源与配置方式.......... 316
11.2.1 路由器的外部配置源........... 316
11.2.2 路由器的配置接口............... 317
11.2.3 路由器与配置终端设备的连接.................................. 318
11.2.4 路由器的配置方式............... 320
11.3 路由器初始化配置...................... 322
11.3.1 使用设置命令工具初始化配置...................................... 322
11.3.2 使用 CLI 命令手动初始配置...................................... 325
11.3.3 使用 Cisco CP Express 初始配置...................................... 327

第 12 章 使用 CLI 配置路由器 ... 339

12.1 路由器配置前的准备................. 339
12.1.1 IP 协议配置原则.................. 339
12.1.2 路由器默认配置 340
12.2 路由器基本配置 342
12.2.1 配置全局参数 342
12.2.2 配置命令行访问 342
12.2.3 配置主机名和密码 343
12.3 配置物理接口 344
12.3.1 接口的一般配置 345
12.3.2 配置以太网接口 346
12.3.3 配置同步串行接口 348
12.4 配置逻辑接口 351
12.4.1 Loopback 接口配置 351
12.4.2 NULL 接口配置................... 351
12.4.3 Tunnel 接口配置.................. 352
12.4.4 Dialer 接口配置 354
12.4.5 子接口配置 355
12.5 配置 PPP 和 MP 协议................. 356
12.5.1 PPP 和 MP 协议概述........... 356
12.5.2 PPP 协议的配置................... 358
12.5.3 MP 协议的配置 360
12.5.4 PPP 的监控.......................... 361
12.6 配置 HDLC 协议 362
12.6.1 HDLC 协议概述 362
12.6.2 HDLC 配置 363
12.7 配置静态路由和默认路由 363
12.7.1 配置静态路由 363
12.7.2 配置默认路由 364
12.8 网络地址转换 364
12.8.1 理解 NAT............................. 365
12.8.2 静态地址转换的实现 367
12.8.3 动态地址转换的实现 367
12.8.4 动态端口地址转换 369
12.9 配置 RIP...................................... 370
12.9.1 RIP 的默认配置 371
12.9.2 配置 RIP 路由 371
12.9.3 配置 RIP 认证 373
12.9.4 配置水平分割 374
12.10 配置 OSPF................................ 375

12.10.1 默认的 OSPF 配置 375
12.10.2 配置基本 OSPF 参数 376
12.10.3 配置 OSPF 接口 377
12.10.4 配置 OSPF 区域参数 378
12.10.5 配置其他 OSPF 参数 379
12.10.6 配置 Loopback 接口 380
12.10.7 监控 OSPF 381
12.11 配置 EIGRP 382
12.11.1 默认的 EIGRP 配置 382
12.11.2 配置基本 EIGRP 参数 383
12.11.3 配置 EIGRP 接口 384
12.11.4 配置 EIGRP 路由认证 385
12.11.5 监控 EIGRP 386

第 13 章 使用 CLI 管理路由器 ... 387

13.1 CF 内存卡的管理........................ 387
13.1.1 需求和限制........................... 387
13.1.2 格式化 CF 卡 388
13.1.3 CF 卡的文件操作................. 389
13.1.4 CF 卡的目录操作................. 392
13.2 系统映像和配置文件的管理...... 393
13.2.1 选择 Cisco IOS 软件版本 393
13.2.2 更新路由器系统映像........... 396
13.2.3 将路由器恢复至出厂默认设置...................................... 400

第 14 章 安全设备概述 403

14.1 网络防火墙................................. 403
14.1.1 网络安全防护的重要意义... 403
14.1.2 网络防火墙简介................... 404
14.1.3 防火墙的主要功能............... 405
14.1.4 防火墙的局限性与脆弱性... 407
14.2 IDS 408
14.2.1 IDS 概述 408
14.2.2 IDS 优势与缺陷 410
14.2.3 IDS 与防火墙联动 412
14.3 IPS 413
14.3.1 IPS 概述 413
14.3.2 IPS 的技术特征 414
14.3.3 IPS 的分类 415
14.3.4 IPS 的优势与作用 417
14.3.5 IPS 的缺陷 418
14.3.6 部署 IPS 419

第 15 章 防火墙的选择与适用 421

15.1 防火墙的主要参数 421
15.1.1 防火墙的性能参数 421
15.1.2 防火墙的功能参数 422
15.2 防火墙的分类与适用 424
15.2.1 按照软硬件形式划分 424
15.2.2 按照实现技术划分 426
15.2.3 按照硬件结构划分 429
15.2.4 按照防火墙在网络中的位置划分 431
15.3 防火墙的选择 431
15.3.1 防火墙的选择策略 432
15.3.2 Cisco ASA 简介 432
15.4 IDS 与 IPS 的选择 435
15.4.1 IDS 的选择........................... 435
15.4.2 IPS 的选择 437

第 16 章 防火墙的端口与连接 439

16.1 防火墙的端口 439
16.1.1 防火墙物理端口 439
16.1.2 防火墙逻辑端口 441
16.1.3 防火墙端口的连接 441
16.1.4 防火墙的 LED 指示灯......... 443
16.2 防火墙的应用环境与连接 447
16.2.1 防火墙连接策略 448
16.2.2 内部网络与 Internet 之间的连接 449
16.2.3 连接局域网和广域网 450

16.2.4 内部网络与第三方网络之间的连接......451
16.2.5 内部网络不同部门之间的连接......452
16.2.6 连接同一部门的不同网络...452
16.2.7 用户与中心服务器之间的连接......453
16.3 IPS 的网络应用与连接......454
16.3.1 路由防护......454
16.3.2 交换防护......454
16.3.3 多链路防护......455
16.3.4 混合防护......456

第 17 章 使用 ASDM 配置管理防火墙 457

17.1 Cisco ASDM 初始化与访问......457
17.1.1 Cisco ASDM 简介......457
17.1.2 Cisco ASDM 初始化......462
17.1.3 配置 Cisco ASDM 访问......465
17.2 Cisco ASDM 配置防火墙......466
17.2.1 DMZ 配置......466
17.2.2 IPsec VPN 远程访问配置....473
17.2.3 Site-to-Site VPN 配置......479
17.3 管理安全设备......482
17.3.1 监视安全设备运行状态......482
17.3.2 查看和分析网络流量......482
17.3.3 查看和分析系统日志......484

第 18 章 使用 CLI 配置管理防火墙 485

18.1 配置的管理与恢复......485
18.1.1 Cisco ASA 默认配置......485
18.1.2 恢复出厂默认配置......489
18.1.3 ASA 配置的保存和管理......489
18.2 配置防火墙和安全环境模式......491
18.2.1 配置透明或路由防火墙......491
18.2.2 配置多环境模式......492
18.2.3 管理安全环境......498
18.2.4 监控安全环境......500
18.3 配置接口......501
18.3.1 接口默认配置......501
18.3.2 配置策略和限制......502
18.3.3 接口配置操作流程......503
18.3.4 将正在使用的接口转换为冗余或 EtherChannel 接口...503
18.3.5 配置和管理冗余接口......505
18.3.6 配置和管理 EtherChannel....507
18.3.7 配置相同安全级别通信......507
18.3.8 配置桥组......507
18.3.9 监视接口......508
18.4 配置 DNS 和 DHCP......509
18.4.1 配置 DNS......509
18.4.2 配置 DHCP......509
18.5 配置对象和访问列表......512
18.5.1 配置对象和组......512
18.5.2 配置扩展访问列表......515
18.5.3 配置 EtherType 访问列表....519
18.5.4 配置标准访问列表......520
18.5.5 配置 Webtype 访问列表......521
18.5.6 配置访问列表日志......523
18.6 配置 NAT......524
18.6.1 ASA 支持的 NAT 类型......524
18.6.2 NAT 规则顺序......524
18.6.3 配置网络对象 NAT......525
18.6.4 配置 Twice NAT......537
18.7 配置访问控制......545
18.7.1 访问规则概述......545
18.7.2 配置和监视访问规则......549

第 1 章　交换机 · 路由器 · 防火墙综述

交换机、路由器和防火墙是几乎所有局域网络都要使用的基本设备。其中，交换机将其他网络设备（如交换机、路由器、网络防火墙、无线接入点）和所有终端设备（如计算机、服务器、网络摄像头、网络打印机）连接在一起，实现彼此之间的通信；路由器用于实现局域网之间，以及局域网与 Internet 的互连，将所有的网络连接在一起；防火墙则用于在内部网络之间，以及内部网络和 Internet 之间创建一个安全屏障，将恶意攻击阻拦在内部网络之外。可见，对于任何局域网络而言，交换机、路由器和防火墙一个都不能少。

1.1　交换机概述

如果把网络布线系统比喻为一条条宽阔的道路，那么，网络交换机（Switch）就像是一座座立交桥，将通往各个方向的道路汇连在一起，实现彼此之间的互连互通。无需红绿灯，无需等待，四通八达，任意驰骋……

1.1.1　交换机的功能

交换机是构建局域网络不可或缺的集线设备。作为局域网通信的重要枢纽和节点，其主要功能就是连接设备。

所谓局域网络（Network），简单地说，其实就是若干计算机的集合，而这些计算机就是借助交换机相互连接在一起的。交换机往往拥有数量众多的端口（通常为 8～52 个端口）。图 1-1 所示为 Cisco Catalyst 2960 系列交换机。

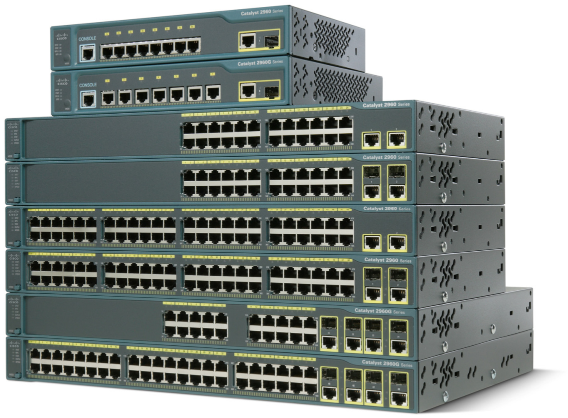


图 1-1　Cisco Catalyst 2960 系列交换机

交换机最主要的功能就是连接计算机、服务器、网络打印机、网络摄像头、IP 电话等终端设备，并实现与其他交换机、无线接入点、网络防火墙、路由器等网络设备的互连，从而构建局域网络，实现所有设备之间的通信。图 1-2 所示为交换机与终端设备和网络设备的连接。

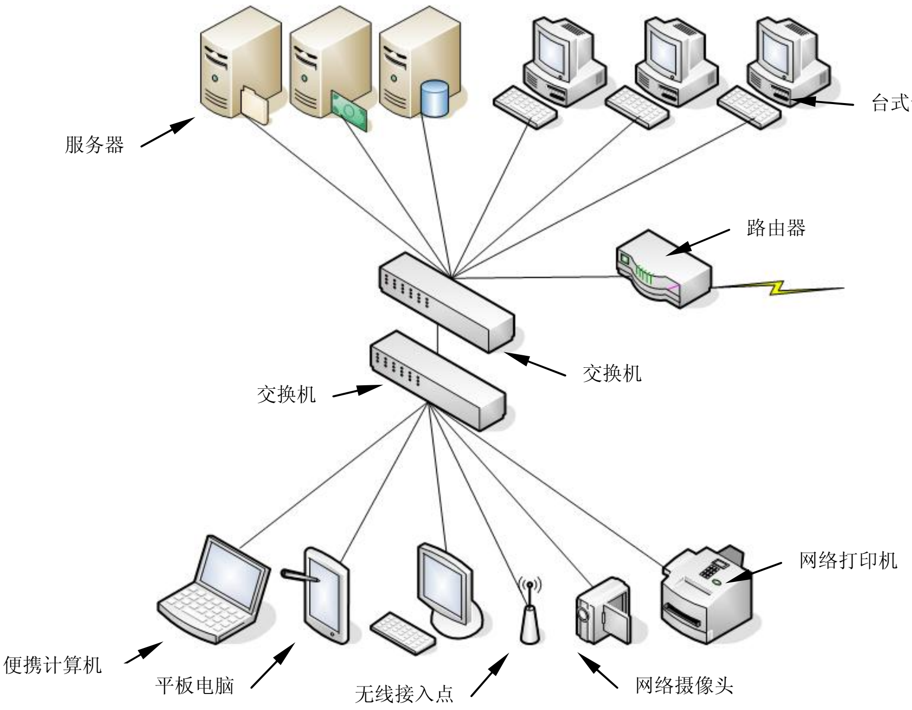


图 1-2　交换机的功能

作为局域网络的核心与枢纽，交换机的性能决定着网络性能，交换机的带宽决定着网络带宽。因此，局域网络的升级往往就是交换机的升级。当然，前提条件是网络布线必须能够满足网络传输的需要。

1.1.2 交换机与交换式网络

可以形象地把计算机比喻为写字楼或工厂，把网络布线比喻为城市马路或高速公路，把网络应用比喻为不同类型的汽车，各种数据则是装在这些汽车上的货物，而交换机就是连接来自所有道路的立交桥。毫无疑问，立交桥都拥有多向多车道，可以从任何一条路转向另外其他一条路，而且所有车辆都可以自行其道，相互之间没有阻碍和影响。

而由交换机构建的局域网络，计算机之间的通信可以同时进行，彼此不受影响干扰，并且每个通信都可以“独享”带宽，即拥有端口所能提供的传输速率。这就好像在限速 80 km/h 的立交桥上，每辆车都可以占用一个车道，都可以跑到 80 km/h 的速率。图 1-3 所示为 6 台计算机同时通信的情形。

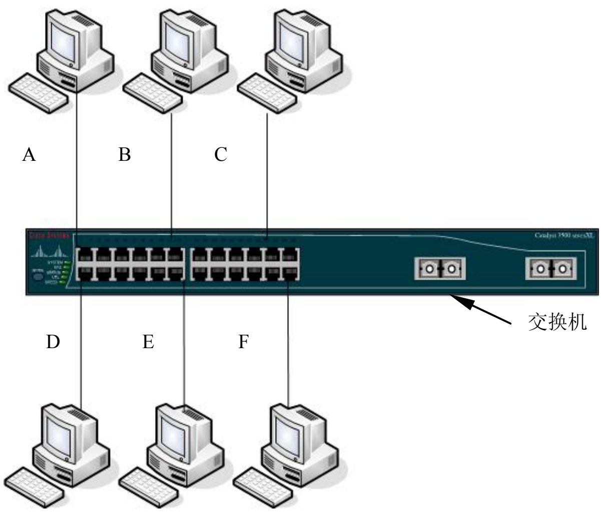


图 1-3　计算机同时通信

由交换机构建的网络称为“交换式网络”。交换式网络的工作模式通常为“全双工”（Full Duplex），即终端设备可以同时接收和发送数据，数据流是双向的（如图 1-4 所示）。对于 100 Mbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 100 Mbps，总带宽即可达到 200 Mbps；对于 1000 Mbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 1000 Mbps，总带宽即可达到 2000 Mbps；同样，对于 10 Gbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 10 Gbps，总带宽将达到惊人的 20 Gbps。

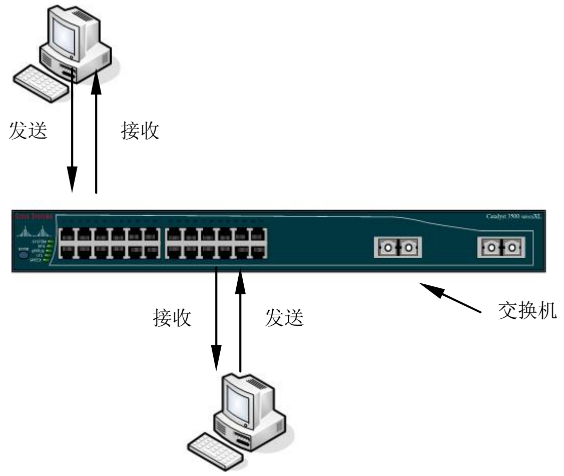


图 1-4　全双工示意图

1.1.3 交换机的工作原理

交换机位于 OSI 参考模型中的数据链路层（即第二层），是一种基于 MAC 地址（Media Access Control，介质访问控制）识别的，用于完成数据的封装和转发的网络设备。交换机可

以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。因此，交换机就像是一个业务熟练的调度员，能够准确地将装载数据的汽车从出发路口直接派送至目的地路口。当然，要完成这样繁重和智能化的工作，交换机也需要一个学习和记忆的过程。

计算机借助网卡连接到局域网络，而每块网卡都有其与生俱来的“胎记”——MAC 地址。交换机通过“学习”，会把连接到每个端口的 MAC 地址记住，形成一个端口与 MAC 地址的对应表。

提·示 MAC 地址是识别局域网节点的标识，所有网络设备（包括每块网卡、交换机和路由器的每个端口）都有一个唯一的 MAC 地址，通常是由网卡生产厂家直接烧入 EPROM 中的，是传输数据时真正用以标识发出数据的设备和接收数据的设备的标志。

交换机的工作过程如下。

（1） 当交换机从某个端口收到一个数据包时，先读取包头中的源 MAC 地址，从而建立源端口与源 MAC 地址的对应关系，并将其添加至地址表。由于交换机能够自动根据收到的以太网帧中的源 MAC 地址更新地址表的内容，所以交换机使用的时间越长，学习到的 MAC 地址就越多，未知的 MAC 地址就越少，因而广播的包就越少（如果目的 MAC 地址未知，则将该包作广播包处理），处理速度就越快。

（2） 读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

（3） 如果地址表中有与该目的 MAC 地址对应的端口，则把数据包直接复制到这端口上。由于不是将该帧发送到所有端口，从而使那些既非源端口又非目的端口的端口间仍然可以进行相互间的通信，进而提供了更高的传输速率。

（4） 如果在 MAC 地址表中没有找到该 MAC 地址，也就是说，该目的 MAC 地址是首次出现，则将该帧发送到所有其他端口（源端口除外），相当于该帧是一个广播帧。拥有该 MAC 地址的网卡在接收到该广播帧后，将立即作出应答，从而使交换机将“端口号-MAC 地址”对照表添加到地址表。

不断重复上述过程，交换机即可实现所有数据的转发，并逐步学习和记忆整个网络中的 MAC 地址，不断丰富和完善自己的 MAC 地址表。

人类的记忆会随着时间的流逝而淡忘。那么交换机是否会永久性地记住所有的端口号－MAC 地址关系呢？答案同样是否定的。由于交换机中的内存有限，因此能够记忆的 MAC 地址数量也是有限的。既然不能无休止地记忆所有的 MAC 地址，那么也必须赋予其相应的忘却机制，从而吐故纳新。事实上，交换机设计了一个自动老化时间（Auto-aging Time）机制，若某 MAC 地址在一定时间内（默认为 300 s）不再出现，那么交换机将自动把该 MAC 地址从地址表中清除。当下一次该 MAC 地址重新出现时，将会被当做新地址处理。另外，由于地址表是保存在内存中的，因此当交换机断电或重新启动后，地址表数据将会全部丢失，必须重新学习。

交换机可以在任意一对端口之间建立临时专用通道，不同端口间的转发可以并行操作。这就像是在各端口间建立起了一座立交桥，形成立体交叉结构，不同流向的数据各行其道，每个端口均能够独享固定带宽，传输速率几乎不受计算机数量的影响。另外，当两个或两个以上的端口与同一目的端口进行通信时，交换机将把这些数据帧暂时保存在缓存中，然后根据顺序

对其逐一处理和转发，从而实现“多”对“一”的通信。

由此可见，交换机的工作过程可以概括为“学习-记忆-接收-查找-转发”。通过广播方式“学习”网卡 MAC 地址，并将“MAC 地址-端口号”的对应关系创建为一个地址表“记忆”在内存中。从源端口“接收”到数据后，在地址表中“查找”与目的 MAC 地址相对应的端口，然后将数据帧“转发”至目的端口。

1.2 路由器概述

路由器用于连接多个网络，以路由器为基础构建（Router Based Network）的网络称为“网间网”。事实上，Internet 就是由数以万计的路由器构建的、超大规模的、国际性的“网间网”。虽然从严格意义上讲，路由器是广域网设备，但是作为局域网实现与其他网络和 Internet 互连的必需设备，也往往被归类于局域网设备之列。

1.2.1 路由器的功能

路由器（Router），顾名思义它是一种智能选择数据传输路由的设备。路由器的端口数量虽然较少，但是种类却非常丰富，可以满足各种类型网络接入的需要。图 1-5 所示为 Cisco 2800 系列路由器及其类型丰富的接口模块。

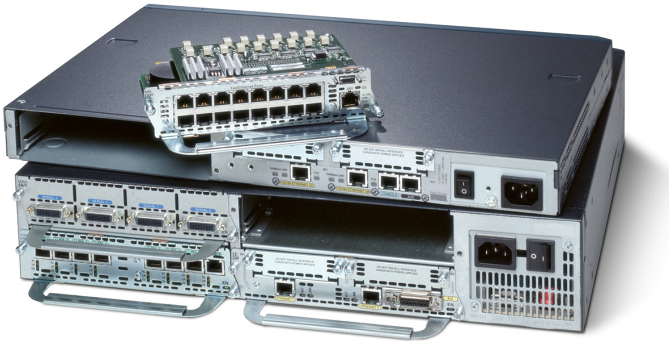


图 1-5　类型丰富的接口模块

1. 连接网络

路由器也称为网关（Gateway）。将局域网络连接在一起，组建更大规模的广域网络，并在每个局域网出口对数据进行筛选和处理，是路由器的重要作用之一。

■　**连接异构网络**

局域网络的类型是多种多样的，除了最常见的以太网外，还有 ATM 网络、FDDI 网络等。异构网络由于分别采用不同的数据封装方式，因此它们之间是无法直接通信的，即使都采用同一种网络协议（比如 TCP/IP 协议，也不能实现彼此间的通信）。而路由器能够将不同类型网络之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方的数据，因此若要实现异构网络间的通信，就必须借助于路由器，如图 1-6 所示。

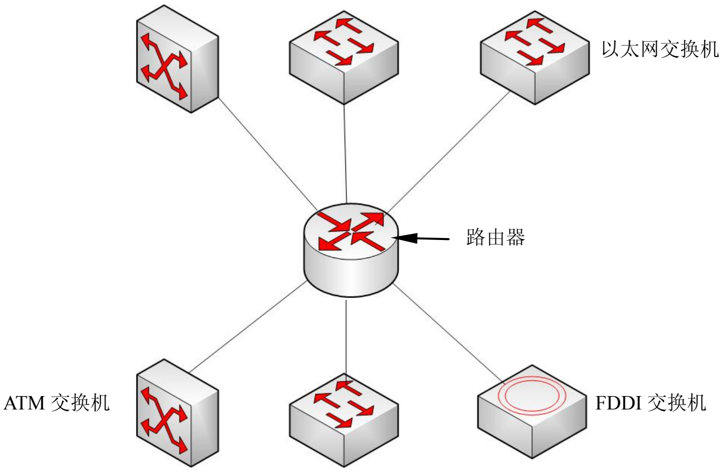


图 1-6　连接异构网络

■　**连接远程网络**

由于局域网的传输距离都非常有限，因此若要实现局域网之间的连接，就必须借助于广域网。相对于局域网而言，广域网无疑是一个异构网络，因此，若要实现局域网之间的远程互连，也必须借助于路由器才能实现，如图 1-7 所示。

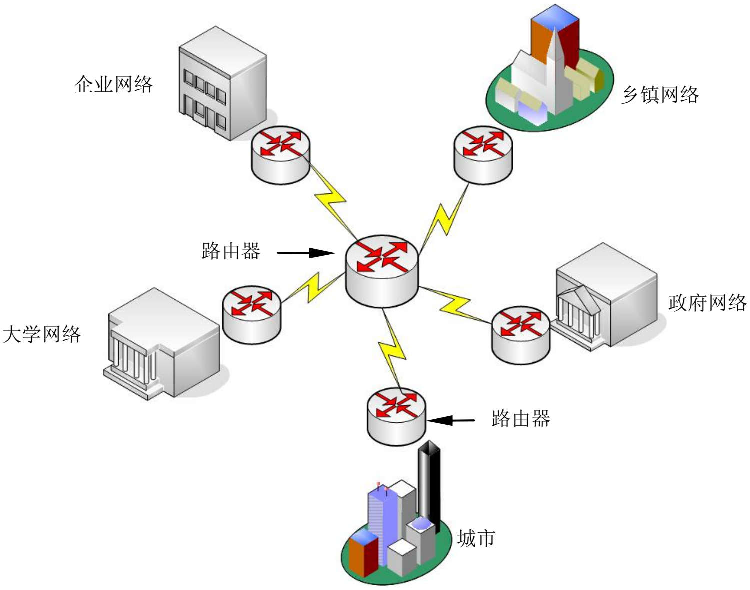


图 1-7　连接远程网络

2.　隔离广播

尽管交换机可以隔离碰撞域，从而提高局域网络的传输效率。然而，交换机却会将所有广播发送至整个网络内所有交换机的每一个端口，而 MAC 地址发现，以及许多网络协议（如 NetBIOS、CDP 等）和网络应用（如 DHCP 服务）等都必须借助广播才能实现。由于广播会发送至网络中的每一个端口，并且由接入网络中的每台计算机进行处理，因此过大的广播量，不仅会严重影响网络的传输效率，而且还会大量占用计算机的 CPU 性能。当有硬件损坏或病

毒攻击时，网络内的广播数量将会剧增，这时将会出现广播风暴，从而使网络传输和数据处理陷于瘫痪。

路由器的重要作用之一就是将广播隔离在局域网内（路由器的每个以太网端口均可视为一个局域网），不会将广播包向外转发（如图 1-8 所示）。因此，大中型局域网都会被人为地划分为若干虚拟网，并使用路由设备实现彼此之间的通信，以达到分隔广播域，提高每个网络的传输效率的目的。

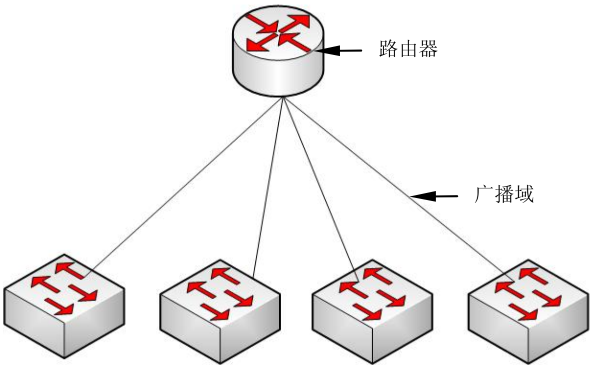


图 1-8　隔离广播域

3. 路由选择

路由器能够按照预先制订的策略，智能选择到达远程目的地的路由。为了实现这一功能，路由器要按照某种路由通信协议，维护和查找路由表。

路由表中列出了整个互联网络中包含的各个节点，以及各节点间的路径情况和与它们相联系的传输费用。如果到特定的节点有一条以上路径，则基于预先确定的准则选择最优（最经济）的路径，如图 1-9 所示。由于各种网络段和其相互连接情况可能发生变化，因此路由信息需要及时更新，这是由所使用的路由信息协议规定的定时更新或者按变化情况更新来完成的。网络中的每个路由器按照这一规则动态地更新它所保持的路由表，以便保持有效的路由信息。

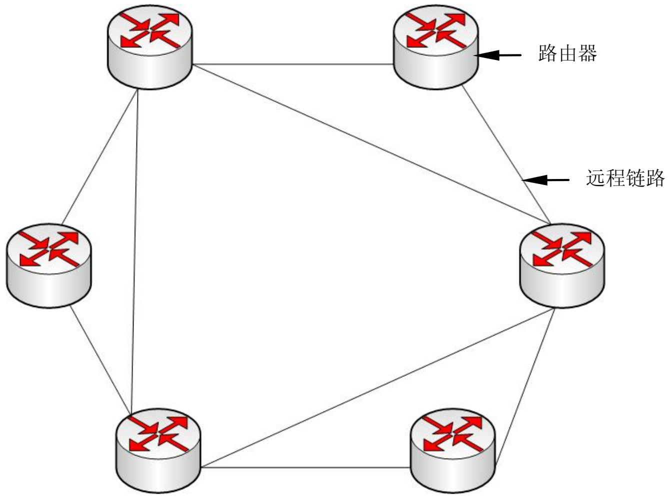


图 1-9　路由选择

4. 网络安全

作为整个局域网络与外界联络的唯一出口，路由器还担当着保护内部用户和数据安全的重要责任。路由器的安全功能主要借助以下两种方式实现。

- 地址转换。局域网内的计算机使用内部保留 IP 地址，这种 IP 地址不能被路由到 Internet，因此不能被外部计算机所知晓，从而可以安全地隐藏在网络内部，避免来自外部的恶意攻击。当内部计算机需要与外部网络通信时，由路由器提供网络地址转换，将其地址转换为合法的 IP 地址，实现对 Internet 的访问。
- 访问列表。借助 IP 访问列表，在路由器上可以设置各种访问策略，规定哪段时间、什么网络协议和哪种网络服务是被允许外出和进入的，从而不仅可以避免对网络的滥用，提高网络传输性能和带宽利用效率，也可以有效地避免蠕虫病毒、黑客工具对内部网络的侵害。

1.2.2 路由器的工作原理

路由器工作于 OSI 参考模型的网络层（即第三层）。路由器通常拥有多个网络接口，分别连接至局域网络（称为局域网端口）和广域网络（称为广域网端口）。每个网络接口分别连接至不同的网络，并分别配置有所连接网络的 IP 地址信息。同时，路由器还维护着一张路由表，记录网络地址与网络端口的对应关系。

1. 路由选择

路由器一个最重要的功能就是选择最佳路由。为此，路由器总是按照一定的规则来动态地更新它所保持的路由表，以便保持路由信息的有效性。

路由器间互通信息进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据量度来决定最佳路径。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一跳（Next Hop）的关系告诉路由器。

路由选择协议通过度量值来决定到达目的地的最佳路径，而小的度量值则代表优选的路径。如果两条或更多路径都有一个相同的小度量值，那么所有这些路径将被平等地分享。通过多条路径分流数据流量被称为到目的地的负载均衡。由于各种网络段和其相互连接情况可能会因环境变化而变化，因此路由情况的信息一般也按所使用的路由信息协议的规定而定时更新。

常见的路由选择协议包括路由信息协议（RIP）、开放式最短路径优先协议（OSPF）和边界网关协议（BGP）等。

2. 数据转发

Internet 用户使用的各种信息服务，其通信的信息最终均可以归结为以 IP 包为单位的信息传送，IP 包除了包括要传送的数据信息外，还包含有信息要发送到的目的 IP 地址、信息发送的源 IP 地址，以及一些相关的控制信息。

当计算机将数据发送给同一网络内的计算机时，源计算机只需将数据发送到网络，目标计算机就能收到。当需要向其他网络的计算机发送数据时，将直接把数据发送到“默认网关（Default Gateway）”，由默认网关负责转发给其他路由设备（如路由器、代理服务器等），直至

将该数据转发至目的计算机所在的网络。也就是说，发送到其他网络的数据先被送到路由器，再由路由器转发出去。

> **提·示** 网络中的设备通过它们的网络地址（TCP/IP 网络中为 IP 地址）相互通信。IP 地址是与硬件地址无关的“逻辑”地址，路由器只根据 IP 地址来转发数据。IP 地址的结构有两部分，一部分定义网络号，另一部分定义网络内的主机号。目前，在 Internet 网络中采用子网掩码来确定 IP 地址中网络地址和主机地址。子网掩码与 IP 地址一样也是 32 bit，并且两者是一一对应的，并规定子网掩码中数字为“1”所对应的 IP 地址中的部分为网络号，为“0”所对应的则为主机号。网络号和主机号合起来，才构成一个完整的 IP 地址。同一个网络中的主机 IP 地址，其网络号必须是相同的，这个网络称为 IP 子网。

与计算机相似，当路由器收到 IP 包时，将根据 IP 包中的目的 IP 地址项查找路由表，根据查找的结果将此 IP 数据包送往对应端口。下一台 IP 路由器收到此 IP 包后继续转发，直至发送到目的地。同时，路由器也有其默认网关，用来传送无法判断目的地的数据包。这样，路由器将已知目的网络的 IP 包正确地转发出去，未知网络的 IP 包传送给“默认网关”路由器，在路由器间重复这项操作，最终将 IP 包传送到目的地。至于那些无法送达目的地的 IP 包，就会被网络自动丢弃。

数据转发即沿最佳路径传送信息分组。路由器的转发过程大致如下。

（1） 接收到 IP 包后，解释并处理该数据包的链路层协议报头，完成对数据的完整性的验证，如 CRC 校验、帧长度检查等。

（2） 根据数据帧中 IP 包头的目的 IP 地址，路由器在路由表中查找下一跳（Next Hop）的 IP 地址。同时，IP 数据包头的 TTL（Time To Live）域开始减数，并重新计算校验和（Checksum）。

（3） 封装上相应的链路层包头，将 IP 包经路由选择的端口转送出去。

1.3 防火墙概述

“防火墙”（Fire Wall）的本意是指发生火灾时，用来防止火势蔓延的一道障碍物，一般都修筑在建筑物之间。而如今的网络防火墙则是指设置在计算机网络之间的一道隔离装置，可以隔离两个或者多个网络、限制网络互访，以保护内部网络用户和数据的安全。

1.3.1 网络防火墙的功能

事实上，网络防火墙更像是企事业单位的门卫制度。各单位借助围墙与外界隔离开来，所有进出人员都必须经过大门，而门卫将对所有人员进行监控和检查，从而保障财产不受损失、人员不受侵害。网络防火墙的作用恰恰也是将内部网络与外部网络分隔开来，对所有进入和外出内部网络的数据进行分析和监控，从而抵御外来非法用户的入侵，并保证内部的重要和敏感数据不致流失。另外，网络防火墙还具有隔离网段、提供代理服务、流量控制等功能，可以满足用户的各种需求。

网络防火墙的功能主要包括以下几个方面。

1. 隔离网络

网络防火墙最基本的功能就是隔离内、外网络，不仅要确保隔离非法用户入侵，更要保证不能使内部信息外泄。因此，网络防火墙通常位于路由器与内部网络（即局域网）之间，使所有进出局域网的数据都能进行过滤和筛选（如图 1-10 所示），从而避免来自外部（主要是 Internet）的网络攻击和欺骗，确保内部网络正常、稳定的运行，以及内部的重要和敏感数据的访问安全。

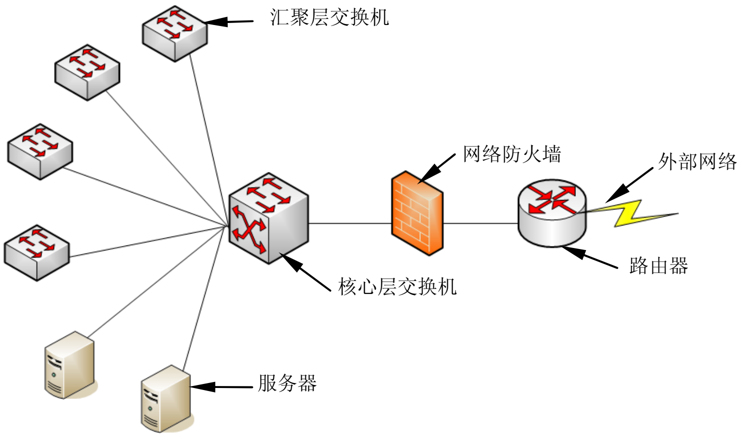


图 1-10　隔离内部和外部网络

除此之外，网络防火墙还被用于隔离内部网络，将一些重要（如总裁办公室、研发中心、网络服务器等）和敏感部门（如人力资源部、财务部等）与普通用户隔离开来，从而避免来自网络内部的恶意攻击，最大限度地保障网络安全，如图 1-11 所示。

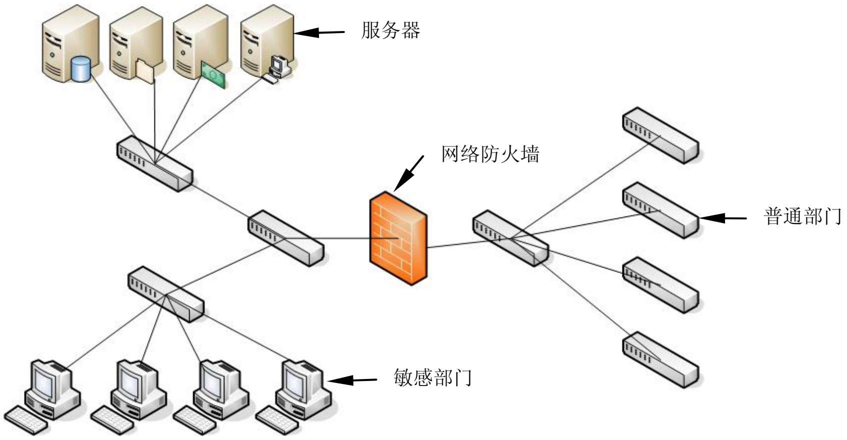


图 1-11　隔离内部敏感网络

2. 保障安全

网络防火墙的安全措施主要包括以下内容。

■ **整合安全策略**

通过以防火墙为中心的安全方案配置，能将所有安全软件（如密码、加密、身份证、审计等）设置在防火墙上。这比将网络安全分散到每个主机上，管理更集中而且更经济。各种安全措施的有机结合，更能有效地对网络的安全性能起到加强作用。

■ **包过滤**

内部网络和外部网络之间的所有网络数据流都必须经过防火墙，只有符合安全策略的数据流才能通过防火墙。包过滤是所有防火墙都具有的基本功能，从 IP 地址、端口判定控制，到判断通信报文协议头的各部分，以及通信协议的应用层命令、内容、用户认证、用户规则甚至状态检测等，都属于包过滤的重要内容。特别是状态监测技术，可以支持多种协议和应用程序，并可以很容易地实现应用层的扩充。

■ **绑定 MAC 地址**

将 MAC 地址与 IP 地址绑定起来，主要用于防止受控（不可访问外网）的内部用户通过更换 IP 地址访问外网。因为更换 IP 地址实现起来太简单了，即使是粗通计算机的人员也能轻松操作，所以绝大多数防火墙都提供了该功能。

■ **流量分析控制**

流量控制可以分为基于 IP 地址的控制和基于用户的控制。基于 IP 地址的控制是对通过防火墙各个网络接口的流量进行控制；基于用户的控制是通过用户登录来控制每个用户的流量，从而防止某些应用或用户占用过多的资源。并且通过流量控制可以保证重要用户和重要接口的连接。流量统计是建立在流量控制基础之上的。一般防火墙可以对 IP、服务、时间、协议等进行统计，并可以与管理界面实现挂接，实时或者以统计报表的形式输出结果。

■ **审计报警机制**

结合网络配置和安全策略对防火墙的相关数据分析完成以后，就要作出接受、拒绝、丢弃或加密等决定。如果要通过防火墙的数据违反了安全策略，审计和报警机制就会开始起作用，并记录和报告。审计是一种重要的安全措施，用以监控通信行为和完善安全策略，检查安全漏洞和错误配置。报警机制是在通信违反相关策略以后，以多种方式（如声音、邮件、电话、手机短信息等）及时报告给管理人员。

3. Internet 共享

借助双向 NAT 技术，网络防火墙可以实现局域网的 Internet 连接共享，使用单一 IP 地址实现内部计算机对 Internet 的访问，并将内部服务器发布到 Internet。

SNAT（Source Network Address Translation，源网络地址转换）用于对内部网络地址进行转换，将内部网络从 Internet 中隐藏起来，使得恶意用户对内部网络的攻击变得更加困难。DNAT（Destination Network Address Translation，目的网络地址转换）主要实现用于外网主机对内网和 DMZ（Demilitarized Zone，隔离区，也称非军事化区）区主机的访问。是一种改变数据包目的 IP 地址的技术，经常和 SNAT 联用，以使多台服务器能共享一个 IP 地址连入 Internet，并且继续服务。通过为同一个 IP 地址分配不同的端口来决定数据的流向，而且还可以将内部服务器发布到 Internet。

提·示 目前，大量的局域网都采用光纤接入城域网。由于 Internet 接入采用的是普通的以太网方式，因此，路由器不再是必需的网络设备，而直接在网络防火墙上设置简单地路由转发，并实现 NAT 转换。当然，对于需要借助长途链路连接到 Internet（如 CERNET）或远程网络的局域网而言，路由器还是不可或缺的设备。

1.3.2 防火墙的工作原理

虽然目前防火墙的基本结构多种多样，但是它们都可以归入包过滤和应用代理两类。其中，包过滤防火墙技术专注的是网络层和传输层，而应用代理防火墙则利用代理服务器，它关心的是应用层的保护。

1. 包过滤防火墙

包过滤防火墙又称作网络级防火墙，工作于 OSI（Open System Interconnect，开放式系统互连）模型的网络层（即第 4 层），通过检查每个数据包的 IP 地址，采用通信协议和端口号等来判断是否允许放行。

防火墙将提取的内部状态信息与其连接状态表进行比较，如果符合其中的某一条规则，就允许数据通过；如果没有符合任何规则，就会使用默认规则进行处理（一般情况下，默认规则就是丢弃该包）。因此，只要定义欲禁止的应用程序所使用的 TCP（Transmission Control Protocol，传输控制协议）或 UDP（User Datagram Protocol，用户数据报协议）端口号，就能阻挡该应用程序或网络服务，不允许其建立特定的连接。

不过，对于那些使用动态端口的应用程序或网络服务而言，这种过滤方式就会发生一些问题。由于防火墙不知道哪些端口需要打开，而用户又必须使用该服务，这就不得不将所有可能用到的端口都打开，而这个范围可能会较大或非常大，从而给黑客以可乘之机。由此，某些防火墙采用动态包过滤技术，通过检查应用程序信息，判断哪些端口需要临时打开。当传输结束以后，这些端口又马上恢复为关闭状态。

网络级防火墙的优点是速度快、费用低、对用户透明。但是其缺点也很突出，即对网络的保护很有限，因为它只检查地址和端口。

2. 应用代理防火墙

应用代理防火墙又称为应用级网关，工作于 OSI 参考模型的应用层（即第 7 层）。该类防火墙类似于代理服务器，可以达到隐藏内部网络结构的作用。其工作过程如下：当客户机需要使用服务器上的数据时，首先将数据请求发给代理服务器，由代理服务器根据这一请求向服务器请求数据。然后再由代理服务器将返回的数据转给客户机。由于外部系统与内部服务器之间没有直接的数据通道，外部的攻击就难以进入到内部企业网。

采用应用代理防火墙有较好的访问控制。但是，当内部网络需要访问外部网络时，同样需要先向代理服务器发送请求。代理服务器根据收到的请求来访问外部网络，并将接收到的数据反馈到内部网络用户。所以，当内部网络用户较多时，经常会出现延迟和多次登录才能访问外

部网络的问题。

可见，应用级防火墙的每一种协议都需要相应的代理软件支持，因此工作量大，且效率较低。令人欣慰的是，结合代理类型防火墙的安全性和包过滤防火墙高速度等优点的自适应代理技术应运而生，由自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet filter）组成，可以在不影响安全性的基础上，将代理型防火墙的性能提高 10 倍以上。只需设置服务类型、安全级别等信息，自适应代理就可以根据用户的配置信息，决定是由代理服务从应用层代理请求还是从网络层转发数据包。

1.4 网络设备在网络中的应用

交换机、路由器和防火墙作为最基本的网络设备，被广泛应用于各种规模的局域网络。其中，交换机作为必不可少的网络设备，将计算机和其他所有网络设备连接在一起。路由器只有在实现 Internet 连接或与其他网络互连时才用得到。网络防火墙并不是必需的网络设备，如果网络对安全性的要求不是太高，也可以不选择。

1.4.1 交换机在网络中的应用

1. 提供网络接口

交换机在网络中最重要的应用就是提供网络接口，所有网络设备的互连都必须借助交换机才能实现。包括：

- 连接交换机、路由器、防火墙、无线接入点等网络设备。
- 连接计算机、服务器等计算机设备。
- 连接网络打印机、网络摄像机、IP 电话等其他网络终端。

图 1-12 所示为大中型网络中交换机与其他设备相连接的拓扑示意图。

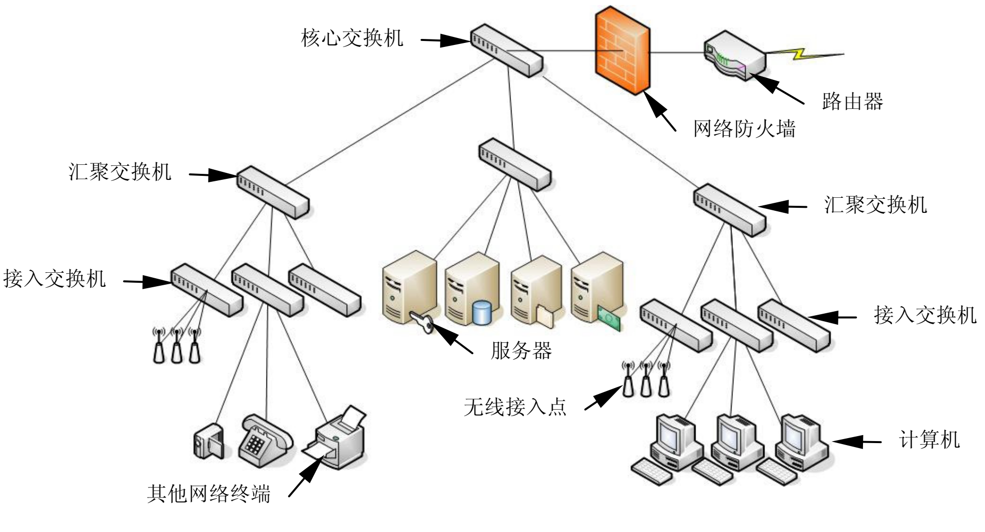


图 1-12 大中型网络中的交换机

需要注意的是，网络拓扑图描述的只是网络设备之间的逻辑连接状况，而这些设备在机柜中的物理安装方式则如图 1-13 所示。

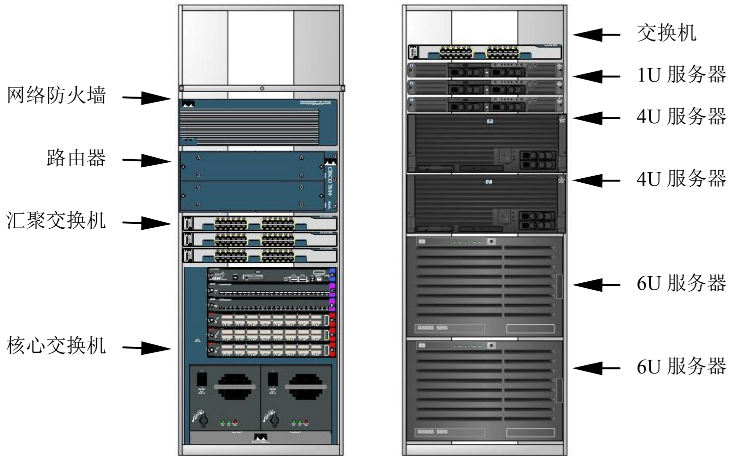


图 1-13 网络设备机架安装示意图

图 1-14 所示为小型网络中交换机与其他设备相连接的拓扑示意图。

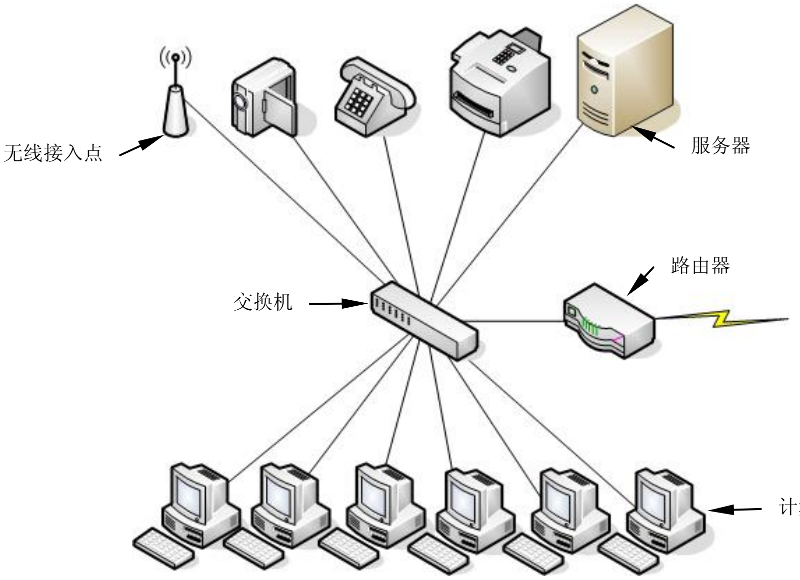


图 1-14 小型网络中的交换机

2. 扩充网络接口

尽管交换机大都拥有较多数量的端口（通常为 8～52 个），但当网络规模较大、接入的计算机数量较多时，一台交换机所能提供的网络接口往往不够。此时，就必须将两台或更多的交换机连接在一起，从而成倍地扩充网络接口。如图 1-15 所示，每台交换机拥有 50 个端口，而将 3 台交换机连接在一起，就可以提供多达 147 个端口（其中 3 个端口被用于彼此之间的级联）。

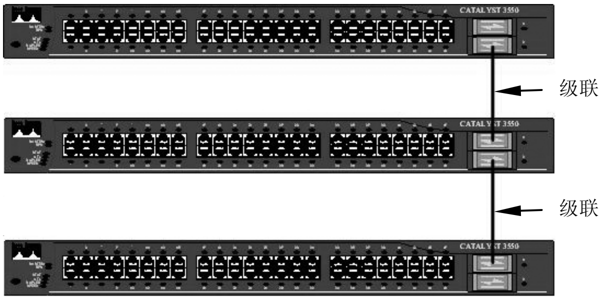


图 1-15　扩充网络接口

3. 扩展网络范围

交换机与计算机或其他网络设备是依靠传输介质（如双绞线、光纤等）连接在一起的，而每种介质的传输距离都是有限的。例如，双绞线是 100 m，多模光纤是 500 m，单模光纤是 2000m。然而，当网络规模较大，需要较远距离的传输时，必须借助交换机进行中继，以成倍地扩展网络覆盖半径。如图 1-16 所示，当只有一台交换机时，双绞线网络的直径为 200 m，而使用光纤连接至另一台交换机后，网络直径就增加至 2200 m。

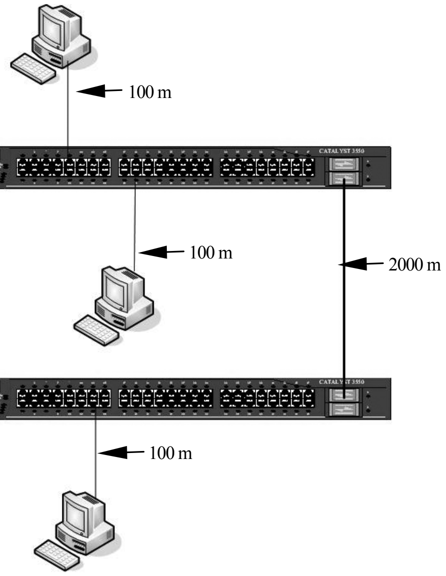


图 1-16　扩展网络范围

1.4.2 路由器在网络中的应用

1. 网络远程连接

随着企业之间的合并，以及办事处或分支机构的不断成立，局域网之间的连接成为一种必要。对于局域网之间的远程连接而言，路由器是不可或缺的设备。图 1-17 所示为 3 个局域

网借助路由器通过远程链路连接在一起。

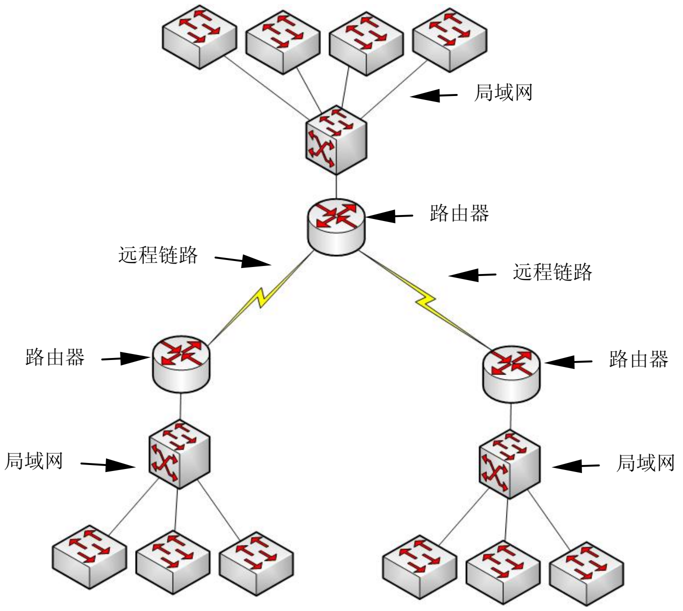


图 1-17　网络远程连接

2.　远程网络访问

当员工在外地出差，或者在家处理一些事务，需要访问公司局域网络内的计算机，或者从公司网络服务器中调取数据时，就需要借助公用链路远程接入公司网络。如图 1-18 所示为普通客户端远程接入公司内部网络。

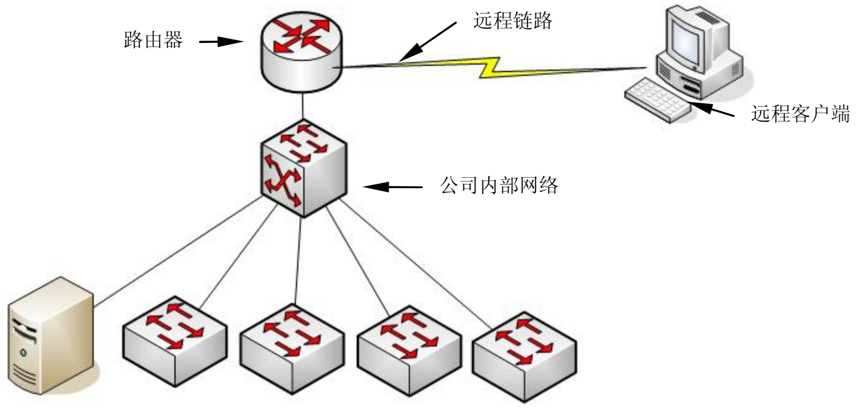


图 1-18　远程网络访问

3.　Internet 连接共享

路由器是局域网络接入 Internet 所必需的网络设备。同时，路由器借助 NAT 技术，只需拥有一个合法的 IP 地址，即可实现局域网的 Internet 连接共享，并实现内部服务器的发布。图 1-19 所示为借助路由器实现局域网的 Internet 连接共享。

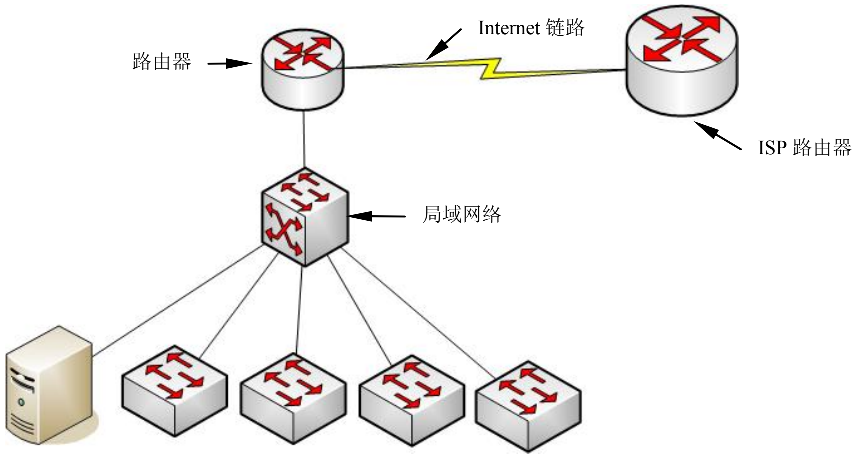


图 1-19　Internet 连接共享

1.4.3 防火墙在网络中的应用

1. 保护网络安全

网络防火墙既可用于分隔内部网络与外部网络，保障内部网络的安全；也可用于分隔内部网络中的重要网络和普通网络，保障重要网络的安全。图 1-20 所示为网络防火墙在大中型网络中的应用。

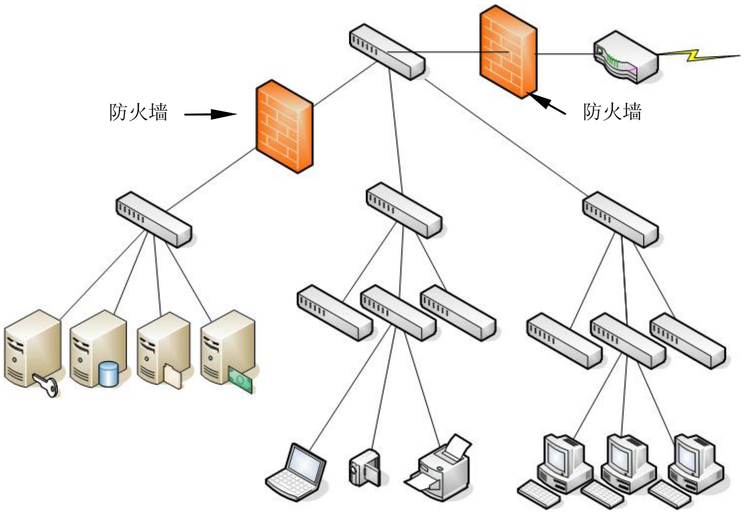


图 1-20　保护网络安全

2. 远程安全访问

网络（如 Internet）中创建安全专用网络通道，实现对内部网络的廉价、安全的远程连接与访问。图 1-21 所示为远程客户端对内部网络的安全访问。

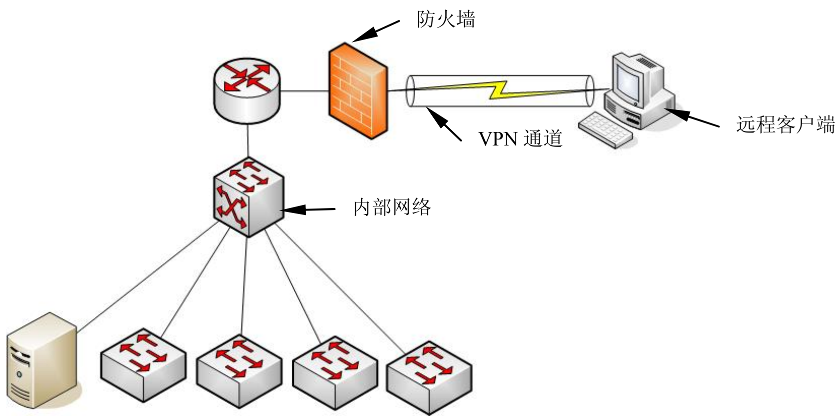


图 1-21　远程安全访问

图 1-22 所示为两个远程网络借助 Internet 建立安全连接。

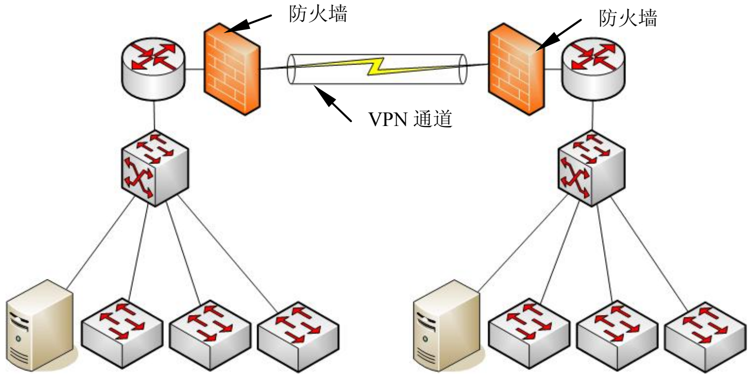


图 1-22　远程安全访问

3. Internet 连接共享

当局域网采用以太网方式连接至 Internet 时，只需借助防火墙（无须路由器）即可实现局域网的 Internet 连接共享（如图 1-23 所示），从而既可保障内部网络的安全，又可将内部服务器发布到 Internet，一举三得。

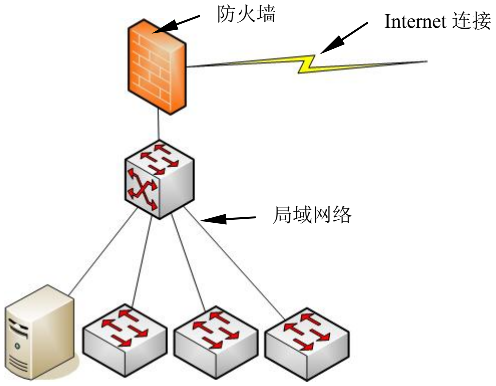


图 1-23　Internet 连接共享

第2章　交 换 技 术

随着交换机技术的不断发展，不仅“千兆位作骨干，百兆位到桌面”的梦想早已成为现实，而且万兆位网络技术也正广泛应用于大中型网络骨干。网络带宽的增加和交换技术的提高，使网络应用更加丰富多彩，视频会议、语音电话正在成为网络新宠，多媒体数据的传输不再受带宽的限制。

2.1　高速以太网技术

随着产品线的不断丰富和价格的不断下降，不仅千兆位以太网已经在各种类型的网络中得到了广泛应用，而且万兆位以太网也已经在大中型网络中得到了普及，十万兆位以太网也正逐渐走进寻常网络。高带宽主干所带来的直接结果是——几乎任何网络应用，甚至包括视频会议、网络电话等对实时性要求较高的网络服务，都能流畅、无阻碍地得以完美实现。

2.1.1　1 Gibt/s 以太网技术

1 Gigabit Ethernet（千兆位以太网）技术是在 100Base-TX 和 100Base-FX 基础上发展起来的超高速网络技术，提供高达 1000 Mbps 的连接速率。该技术一经提出就得到了网络界人士的普遍关注，使得曾经被业界一致公认的网络主干升级技术 ATM 失去了原有的吸引力而消失。

1.　千兆位以太网的主要特点

千兆位以太网具有以下主要特点。

■　**简易性**

千兆位以太网继承了快速以太网的简易性，因此其技术原理、安装实施和管理维护都很简单。另外，千兆位以太网支持新的全双工操作模式，在一对线上可以同时用于发送和接收信息，因此无需采用 CSMA/CD 机制。数据传输在不同的线对进行，传输之前无需再等待，没有了冲突的发生，从而在点对点交换链路中可以提供更宽的带宽。

■　**扩展性**

由于千兆位以太网采用了快速以太网的基本技术，原有的布线系统也几乎完全支持，因此，由 100Base-TX/100Base-FX 升级到 1000Base-T/1000Base-SX/1000Base-LX 等千兆位以太网非常容易，而且两种技术可以在同一网络中和谐共存、同时使用，使得网络升级和扩展变得更加简单。

■　**可靠性**

由于千兆位以太网保持了快速以太网的安装维护方法，借助网络设备的 LED 指示灯就能

够快速诊断和排除大量的网络故障。同时，可以采用星型、网状、环型等网络拓扑结构，因此网络具有很高的可靠性。

■ **经济性**

千兆位以太网已经被广泛应用，所有网络厂商都生产千兆位以太网产品，几乎所有的交换机都支持千兆位以太网端口，千兆位以太网设备上已经没有多少技术含量可言，市场竞争也已经非常充分，因此，千兆位以太网设备的价格也变得平易近人。

■ **可管理维护性**

千兆位以太网采用基于简单网络管理协议（SNMP，Simple Network Management Protocol）和远程网络监视（RMON，Remote Network Monitoring）等网络管理技术，许多软硬件厂商开发了大量的网络管理软件，使千兆位以太网的集中监控、管理和维护变得非常简便。

■ **广泛应用性**

千兆位以太网为局域主干网和城域主干网提供了一种高性价比的宽带传输交换平台，使得许多宽带应用能够得以施展其魅力。例如，在千兆位以太网上可以流畅地实现视频点播、现场直播、教学观摩等大码流的网络服务和应用。

2. 千兆位以太网应用方案

千兆位以太网联盟（Gigabit Ethernet Alliance，GEA）为千兆位以太网的应用提出以下几种具体方案。

■ **网络主干升级**

在不对原有传输光缆作任何改变的情况下，只需将网络中心交换机由原来的快速以太网交换机更换为千兆位以太网交换机，即可将局域网络的主干提升至千兆位，从而全面改善原有的网络性能，不仅简单、易行、投资小，而且网络从此将变得畅通无阻。

■ **服务器链路升级**

将安装有千兆位以太网卡的服务器直接与千兆位以太网交换机进行连接，全面升级服务器至交换机的通信链路，为服务器提供无阻塞的、千兆位线速交换能力，为实现网络的多媒体应用奠定基础。无论采用光缆连接，还是非屏蔽双绞线连接，都不会有太大的投入，但都将使局域网络的服务质量迈上一个新的台阶，并为局域网络的多媒体传输和应用奠定坚实的基础。

■ **升级交换机之间的连接**

一旦主干传输（核心层交换机与汇聚层交换机间的连接）速度提高到了 1 Gbps，接入层传输（汇聚层交换机与接入交换机间的连接）自然就成为下个升级的目标。选择提供 1000 Mbps 端口或模块的接入交换机，或者索性采用端口全部为 1000 Mbps 的接入交换机都是简捷的升级方法。

■ **千兆位到桌面**

高性能工作站（如图形工作站、3D 工作站等）安装千兆位以太网卡，直接与千兆位以太网相连，从而实现桌面计算机与局域网络的的千兆位连接。尽管品牌计算机几乎都提供了千兆位以太网接口，不过，就目前的网络应用而言，普通的网络客户端似乎还没有必要采用千兆位

以太网接入。

如图 2-1 所示，局域网络的所有连接可以全部采用千兆位带宽。

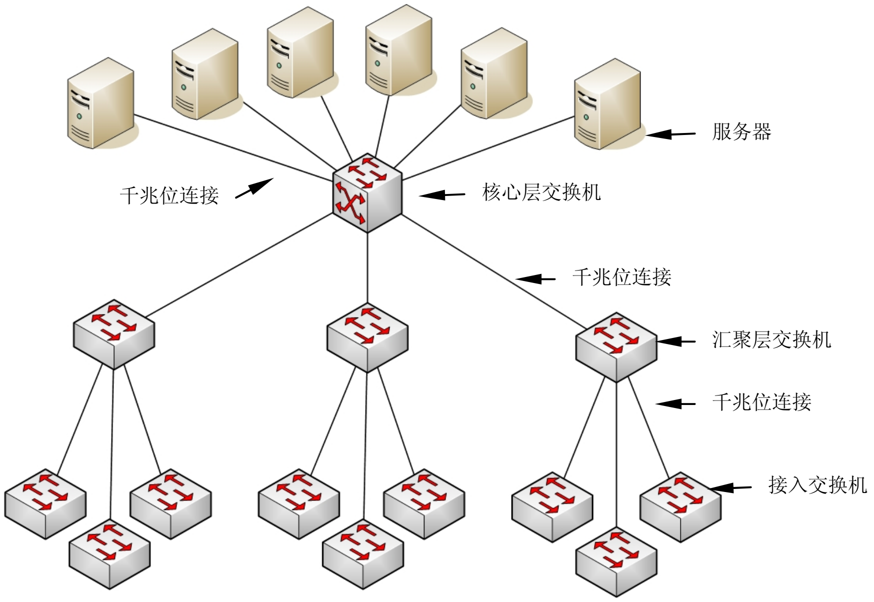


图 2-1　千兆位连接应用

2.1.2 10 Gbit/s 以太网技术

10 Gigabit Ethernet（万兆位以太网）技术已经成熟，并且被广泛应用于新搭建的高性能局域网络，或者被用于原有网络的升级和改造。不过，由于 10 Gbps 设备的价格仍然较为昂贵，因此目前大多被应用于网络主干链路。

1. 万兆以太网技术特点

万兆位以太网相对于千兆位以太网拥有许多的优势和特点。

■ **结构简单**

万兆位以太网结构简单、管理方便。万兆位以太网是一种只采用全双工的技术，其物理层（PHY，Physical Layer）和 OSI（Open System Interconnect，开放式系统互连）参考模型的第 1 层（物理层）一致，负责建立传输介质（光纤或铜线）和 MAC（Media Access Control，介质访问控制）层的连接。MAC 层相当于 OSI 参考模型的第二层（数据链路层）。在网络的结构模型中，把 PHY 进一步划分为物理介质关联层（PMD，Physical Media Dependent）和物理代码子层（PCS，Physical Coding Sublayer）。光学转换器属于 PMD 层。PCS 层由信息的编码方式（如 64B/66B）、串行或多路复用等功能组成。由于没有采用访问优先控制技术，简化了访问控制的算法，从而简化了网络的管理，并降低了部署的成本，因而得到了广泛的应用。

■ **技术兼容**

万兆位以太网技术基本承袭了快速以太网和千兆位以太网技术，因此在用户普及率、使

用方便性、网络互操作性及简易性上皆占有极大的引进优势。在升级到万兆位以太网解决方案时，用户不必担心既有的程序或服务是否会受到影响，升级的风险非常低，同时还拥有在未来升级到 100 Gbps 的潜力。

以太网的可平滑升级保护了用户的投资。以太网的改进始终保持向前兼容，使得用户能够实现无缝的升级，既不需要额外的投资升级上层应用系统，也不影响原来的业务部署和应用。

■ **宽带更高**

万兆位标准意味着以太网将具有更高的带宽（10 Gbps）和更远的传输距离（最长传输距离可达 40 km）。过去有时需采用数个千兆位捆绑以满足交换机互连所需的高带宽，因而浪费了更多的光纤资源，现在可以采用万兆位互连，甚至 4 个万兆位捆绑互连，达到 40 Gbps 的带宽水平。

随着网络应用的深入，WAN/MAN 与 LAN 融合已经成为大势所趋，各自的应用领域也将获得新的突破，而万兆位以太网技术让业界找到了一条能够同时提高以太网的速度、可操作距离和连通性的途径，万兆位以太网技术的应用必将为三网融合提供新的动力。

■ **易于管理**

万兆位以太网技术提供了更多和更新的功能，能够更好地满足网络安全、服务质量、链路保护等多个方面需求。网络管理者既可以用实时方式，也可以用历史累积方式轻松查看第二层到第四层的网络流量。“永远在线”监视能够及时进行入侵监测，发现网络性能瓶颈，获取计费信息或呼叫数据记录，从而使得网络管理更加简单、准确和有效。

2. 万兆位以太网应用领域

万兆位以太网应用领域主要包括以下几方面。

■ **交换机之间互连**

过去，必须采用多个千兆位捆绑，以满足交换机互连所需的高带宽。现在，可以采用万兆位实现核心层交换机与汇聚层交换机的互连，甚至是汇聚层交换机与接入交换机之间的互连（如图 2-2 所示）。同时，根据现实的需要，还可以将 4 个 10 Gbps 链路捆绑在一起，从而达到 40 Gbps 的网络带宽。

■ **数据中心或服务器群组带宽汇聚**

视频服务器、应用服务器、邮件服务器、文件服务器、数据库服务器等网络服务器所需要的数据带宽是非常可观的，因此，将服务器与主干网络的连接带宽升级到万兆位，将大幅提高网络服务器的服务质量。

■ **城域网带宽汇聚与骨干更新**

在城域网的建设中，接入层会有越来越多的万兆位或千兆位以太网连到城域网的汇聚层，而汇聚层也会有越来越多的千兆位以太网连到城域网的骨干层，从而使得万兆位或万兆位捆绑技术在城域网中的汇聚层及骨干层中成为必要。

■ **宽带广域网**

由于以太网的价格优势，而万兆位以太网又支持与 SONET（Synchronous Optical Network，同步光纤网络）/SDH（Synchronous Digital Hierarchy，同步数字体系）基础架构的无缝连接能力，这使得万兆位以太网方案将在广域网市场中取得一定的发展。就目前的成本和需求来看，

100 Gbit/s 以太网的商用在城域网先行是比较可行的方案。在城域网中，大量的数据需要随时的上下路，一个无需各种补偿器件的传输系统将会大大简化网络设计，100 Gbit/s 以太网刚好可以满足这一需求，同时高带宽满足了城域网每年 40%的流量增长。总之，100 Gbit/s 以太网的发展需求已经很明显，成本优势也会不断加强，但是 100 Gbit/s 以太网传输从调制方式到运营管理维护都需要不断的技术完善，真正大规模的商用还需时日。

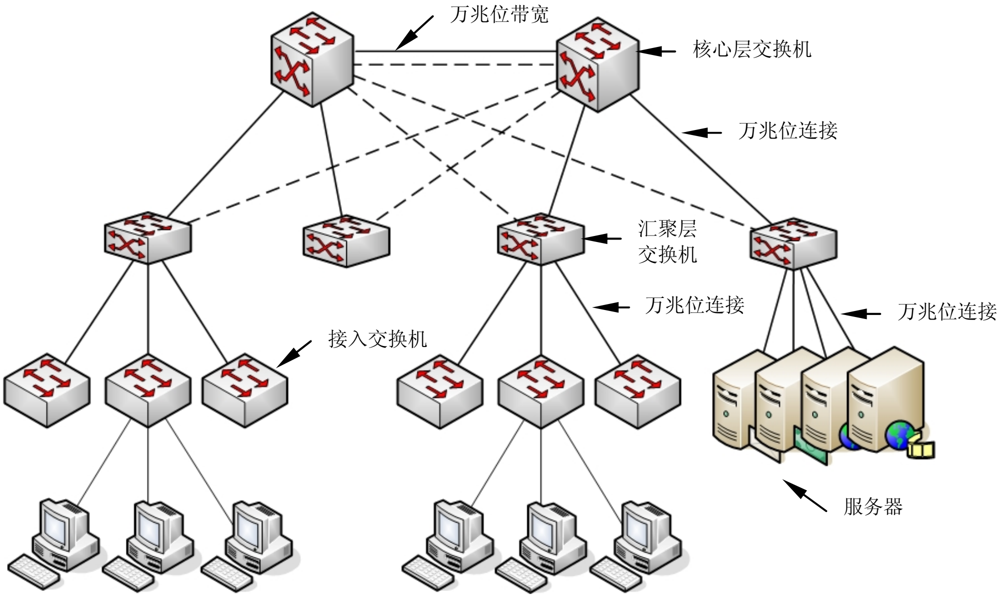


图 2-2　万兆位连接应用

■　**存储网络**

万兆位以太网不仅可以满足存储设备的高速互连，也可以实现存储设备的备份及灾难恢复。由于存储网络对网络带宽的需求较高，因此，万兆位以太网在存储网络的应用上得到了充分的发挥（如图 2-3 所示）。

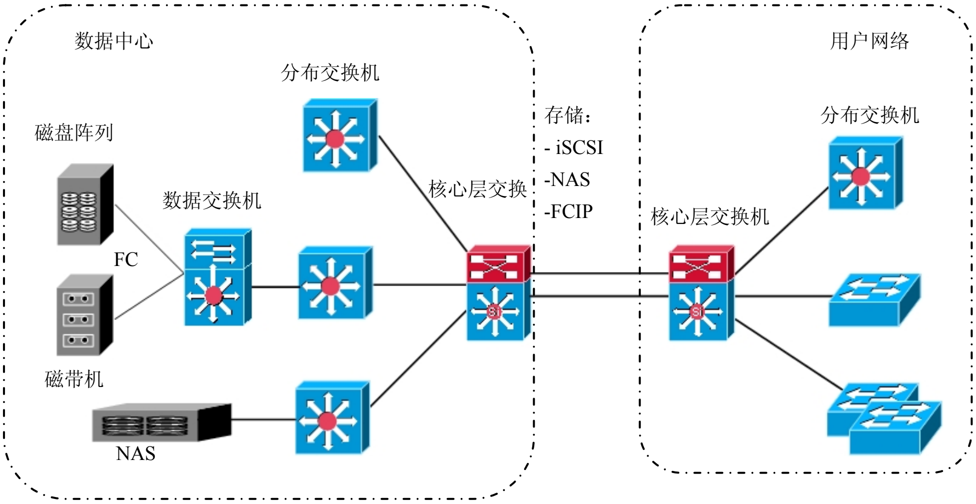


图 2-3　万兆位存储网络

■ **高性能计算应用**

研究机构可以将很多独立的高速 CPU 连接到一起，利用万兆位以太网或者万兆位以太网通道连接传输大量的处理器间通信，这对于确保一个大规模的分布式超级计算机集群的最佳性能至关重要。

从国内市场来看，教育科研网络、电信运营商及存储网络已经广泛采用了万兆位以太网技术。

2.1.3 40/100 Gbit/s 以太网技术

40 Gigabit Ethernet（4 万兆位以太网）技术已经被应用于高性能核心交换机和数据中心交换机，而 100 Gigabit Ethernet（十万兆位以太网）技术也已经在云计算、虚拟化等高端交换机中崭露头角。

1. 40/100 Gbit/s 以太网技术特点

下一代以太网技术标准包含了 40 Gbit/s 和 100 Gbit/s 两种速度，主要针对服务器和网络方面不同的需求。40 Gbit/s 主要针对计算应用，而 100 Gbit/s 则主要针对核心和汇接应用。提供两种速度，IEEE 意在保证以太网能够更高效更经济地满足不同应用的需要，进一步推动基于以太网技术的网络会聚。标准规定了物理编码子层（PCS）、物理介质接入（PMA）子层、物理介质相关（PMD）子层、转发错误纠正（FEC）各模块及连接接口总线，MAC、PHY 间的片间总线使用 XLAUI（40 Gbit/s）、CAUI（100 Gbit/s），片内总线用 XLGMII（40 Gbit/s）、CGMII（100 Gbit/s）。

■ **保留以太网帧格式**

40/100 Gbit/s 以太网仅支持全双工操作，保留了 802.3MAC 的以太网帧格式；定义了多种物理介质接口规范，其中有 1 m 背板连接（100GE 接口无背板连接定义）、7 m 铜缆线、100 m 并行多模光纤和 10 km 单模光纤（基于 WDM 技术），100 Gbit/s 接口最大定义了 40 km 传输距离。标准定义了 PCS 的多通道分发（MLD）协议架构，标准还定义了用于片间连接的电接口规范，40 Gbit/s 和 100 Gbit/s 分别使用 4 个和 10 个 10.312 5 Gbit/s 通道，采用轮询机制进行数据分配获得 40G 和 100G 的速率，另通过虚拟通道的定义解决了适配不同物理通道或光波长问题；明确了物理层编码采用 64B/66B。

■ **可利用现有布线系统**

新一代以太网标准在制订时，已经充分考虑了电接口相关标准和技术的成熟情况，采用了 10.312 5 Gbit/s 的片间互联传输通道，多模的并行光纤接口可以支持在 OM3 光纤满足 100 m 甚至更远的距离；单模的 40GB ASE-LR4 使用粗波分复用（CWDM）经济可行，100GB ASE-LR4 使用 DWDM，每波长传 25.781 25 Gbit/s，使用 1 295～1 310 nm 波长，完全可以使用原有光纤，综合技术和成本，标准选用的技术都是实用可行的，有助于促进 100G 接口在局部和城域网范围内商用。

■ **可实现网络平滑升级**

对于全网范围的使用，串行 100GE 传输标准和技术成熟前，可采用反向复用技术。将 10×

10GE 或者 4×25GE 接口的 100GE 业务经 ODU2/ODU3 适配到 OTU2/OTU3，在 10G/40G 光网络中通过多个波长进行传输。可以不需对现存的 10G/40G DWDM 光网络进行重新设计与改动，传输码型仍然为光双二进制编码（ODB）/差分归零码（DRZ）/电归零码－差分正交相移键控（eRZ-DQPSK）。这种模式可以采用 10G/40G 现有的成熟光电器件，并且整个系统的性能指标和 10G/40G 系统一致。这一方案可实现网络平滑升级，满足运营商的成本期望，并且器件相对成熟。

2. 40/100 Gbit/s 以太网应用领域

随着 IT 行业的高速发展，云计算、虚拟化、高清视频、电子商务、社交网络以及飞速发展高速无线网络等各种新兴业务的不断涌现，都给基础网络带来了巨大的机会和挑战。对于汇聚层的应用，下行端口正在切换到 10 Gbit/s，上行只能采用 10 Gbit/s 端口的链路聚合，如果使用 100 Gbit/s 以太网接口则可以在数据流的管理、分配及效率上得到改善；对于数据中心，随着 10 Gbit/s 接口增加也同样存在上行及内部互联高速接口的需求；对于骨干网的高效传输，也期待着 100 Gbit/s 高速接口和传输的成熟。

■ 网络骨干带宽提升

从网络的架构来看，网络的扁平化和融合也都大大促进了 40 Gbit/s、100 Gbit/s 高速接口的发展。网络的扁平化对核心交换机提出了更高端口密度和更高速率上行接口的要求，如每槽位需要 32 个 10 GE 接口。在如此高密度、大容量的接入带宽下面，上行接口的带宽就有了更高的需求。比较常见的部署就是用多个 10 Gbit/s 端口进行聚合和捆绑，来实现更高性能的上行接口。可见，40 Gbit/s、100 Gbit/s 的接口需求不仅是现实的，而且是迫切的。

■ 城域网业务汇聚

随着网络应用的不断丰富，如文件下载与系统更新、电子银行与在线购物、高清影视直播与视频会议等，使得用户的带宽需求从 1 Mbps 迅速上升到 10 Mbps、100 Mbps，甚至 1000 Mbps。随着以视频业务为代表的宽带业务的快速发展，接入层带宽的增加必然导致城域网汇聚层和核心层的宽带需求增加。有数据表明，10 Gbps 端口的增长速度已远远高于低速端口的增长速度，在接入和客户端设备上 10 Gbps 端口的应用正越来越多，在此趋势下，汇聚层节点数量以及带宽的快速攀升，而这势必会引发网络汇聚层和骨干层对 40 Gbps、100 Gbps 端口需求的迅速增长，从而促使运营商在城域网核心层部署 100 Gbit/s，以适应大带宽业务流量汇聚以及与长途传输设备接口之需。

■ 数据中心网络

随着数据中心网络建设的融和趋势，局域网、存储网络和高性能计算网络融正逐步统一到以太网接口上，这也大大增加了服务器对 10 Gbit/s、40 Gbit/s 以太网接口的需求。一旦 10 Gbit/s、40 Gbit/s 接口成为服务器的普及端口，数据中心内部 40 Gbit/s、100 Gbit/s 的互联交换机接口就变得十分必要和紧迫。不仅如此，超大型的数据中心往往有很大的地域跨度，这些数据中心的互联以及同 Internet 的接入都需要更高速率的链路。

在数据中心将众多服务器集中在一起的服务模式下，100 Gbit/s 技术的采用，不仅可以满足数据中心互联的海量带宽需求，而且可以有效减少接口，降低机房占地面积以及设备功耗，帮助运营商以及互联网企业部署高密度、万兆互联的新一代数据中心。

■ **云计算**

带宽压力是云数据中心网络的核心问题。在数据中心，像视频点播、10 Gbit/s 的 FCOE、以及高性能计算这样的高带宽应用，都需要万兆以太网接口。随着服务器和接入设备上万兆以太网的普及，数据中心的网络汇聚层和核心层设备对 100 Gbit/s 以太网的需求越来越强烈。100 Gbit/s 网络不仅仅意味着端口、带宽速度的升级，不只是在数据传输速率上比 10 Gbit/s 快了 10 倍，更重要的是由此带来的功能上的极大增强和丰富。作为新一代的云数据中心，必将在其汇聚层或核心层采用 100 Gbit/s 以太网以满足应用需求，云数据中心将进入 100 Gbit/s 时代。

■ **远程网络互联**

在网络 IP 化趋势下，骨干网的数据流量主要由核心路由器产生。现在网络中核心路由器主要采用 10 GE 接口与 WDM 设备互联以实现长距离传输。随着 100 Gbit/s 技术的成熟，核心路由器可以直接采用 100 Gbit/s 接口与传输设备相连，不仅可以实现大容量和高带宽，还可以进一步减少用户侧接口数量，以满足数据业务发展的需要。目前，由于 100 Gbit/s 接口已经被公认为是下一代核心路由器的标准配置，国内外的各大设备厂商竞相推出了 100 Gbit/s 的产品和设备。

相对而言，40 Gbit/s 端口的相关技术和产业链相对成熟，在芯片成本、光模块成本和端口部署等方面都有着非常现实的意义，可以很快实现规模性的应用，而 100 Gbit/s 虽然在诸多方面都存在技术和成本问题，但是，却代表着高速以太网未来发展的方向。就目前市场定位来看，两者各有所侧重，40 Gbit/s 以太网主要面向数据中心的应用，而 100 Gbit/s 以太网则更侧重在网络汇聚和骨干。

总之，为了更好地应对业务流量和网络带宽增长的压力，具备大容量、长距离传输特征的 100 Gbit/s 技术正在被越来越多地部署到干线网络、大型本地网以及城域网的核心层，用于城域网业务流量汇聚、大型数据中心之间的数据交互、核心路由器之间的接口互联以及大容量长距离传输等多种场景，为网络的新一轮提速奠定基础。

2.2 虚拟网技术

随着网络内计算机数量的增多，广播包的数量也会急剧增加。当广播包的数量占到通信总量的30%时，网络的传输效率将会明显下降。所以，当局域网内的计算机达到一定数量后（通常限制在 200 台以内），通常采用划分虚拟网（Virtual Local Area Network，VLAN）的方式将网络分隔开来，将一个大的广播域划分为若干个小的广播域，以减小广播可能造成的损害，子网之间进行通信也必须通过路由设备。

2.2.1 虚拟网的意义和作用

在局域网络中使用 VLAN 技术，具有以下重要意义和作用。

- 降低移动和变更的管理成本。VLAN 中的成员与其物理位置无关，既可连接至同一台交换机，也可连接至不同交换机。当需要把一台计算机从一个子网转移到另一个子网时，迁移工作只是由网络管理员以远程管理的方式，在相应的交换机上将指定端口重新定义一下 VLAN 成员即可。

- 控制广播。由于所有的广播都只在本 VLAN 内进行，而不再扩散到其他 VLAN 上，所以将大大减少广播对网络带宽的占用，提高网络传输效率，并可有效地避免广播风暴的产生。
- 增强安全性。VLAN 的一个重要特性就是提高了网络安全性。由于交换机只能在同一 VLAN 内的端口之间交换数据，不同 VLAN 的端口不能直接相互访问，只能通过三层交换或路由才能访问。因此通过划分 VLAN，就可以在逻辑上防止某些非授权用户访问敏感数据。
- 网络监督和管理的自动化。由于网络管理员可以通过网管软件，查看 VLAN 间和 VLAN 内通信的数据报的细目分类信息，以及应用数据报的细目分类信息，而这些信息对于确定路由系统，和经常被访问的服务器的最佳配置十分有用。通过划分 VLAN，可以使网络管理变得更简单、更轻松、更有效。

VTP（VLAN Trunking Protocol）是一种消息协议，用于在 VTP 域内同步 VLAN 信息（VLANs 的添加、删除和重命名），而不必在每个交换机上配置相同的 VLAN 信息，从而实现 VLAN 配置的一致性。使用 VTP，可以在一个或多个交换机上建立配置修改中心，并自动完成与网络中其他所有交换机的通信，可以有效地减少交换网络中的管理事务。

2.2.2 虚拟网的类型与适用

当在交换机上划分 VLAN 后，不同 VLAN 间的设备就如同被物理地分隔开来。也就是说，连接到同一交换机，然而处于不同 VLAN 的设备，就像是被物理地连接到两个位于不同网段的交换机上一样，彼此之间的通信一定要经过路由设备，否则将无法得知对方的存在，将无法进行任何联系。

1. 基于端口的 VLAN

基于端口的 VLAN 是最常使用的划分 VLAN 的方式，被所有的以太网交换机所支持。所谓基于端口的 VLAN，是指由网络管理员借助网管软件远程或者直接连接到交换机，将某些端口直接地、强制性地分配给某个 VLAN（如图 2-4 所示）。除非网管人员重新设置，否则这些端口将一直保持对该 VLAN 的从属性，即属于该 VLAN，因此这种 VLAN 划分方式也称为静态 VLAN。

这种 VLAN 划分方法，虽然在网络管理员进行初始 VLAN 划分操作时会比较麻烦，但相对安全，并且容易配置和维护。同时，由于不同 VLAN 间的端口不能直接相互通信，因此每个 VLAN 都有自己独立的生成树。此外，交换机之间在不同 VLAN 中可以有多个并行链路，以提高 VLAN 内部的交换速率，增加交换机之间的带宽。

需要注意的是，不仅可以将同一交换机的不同端口划分为同一 VLAN，而且还可以设置跨越交换机的 VLAN（如图 2-5 所示），即将不同交换机的不同端口划分至同一 VLAN，这就完全解决了位于不同物理位置、连接至不同交换机中的用户如何使之处于同一 VLAN 的难题。例如，在一个拥有数十台、甚至数百台计算机的企业办公网中，为了提高网络传输效率，可以将所有用户划分为行政、销售、研发、生产、售后、财务等多个 VLAN。虽然各部门位于不同的建筑物内，连接至不同的交换机，但仍然能够根据其连接的端口将其划分至同一 VLAN，实现彼此之间的正常通信。

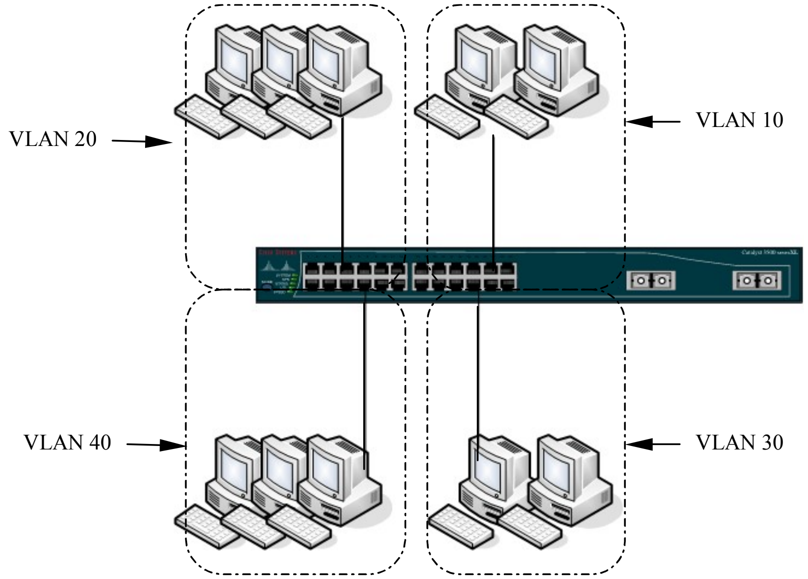


图 2-4　基于端口的 VLAN

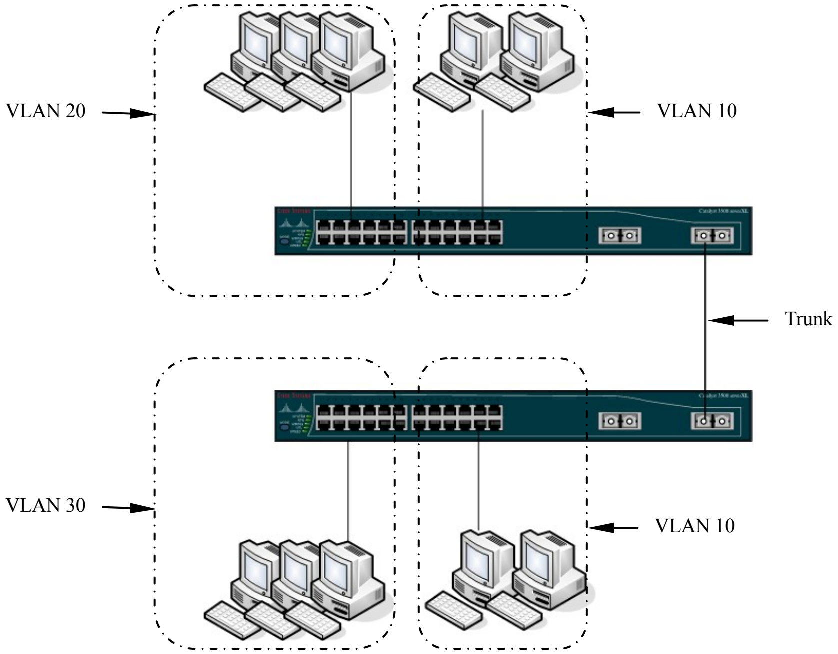


图 2-5　VLAN 与 Trunk

不仅不同交换机上具有相同 ID 的 VLAN 之间，可以借助一条链路实现彼此之间的连接。而且，不同交换机之间也可以借助一条链路同时传输多个 VLAN，实现 VLAN 内部的相互通信。用于连接不同 VLAN 的链路，称之为 VLAN 中继（VLAN Trunk）。

2.　基于 MAC 的 VLAN

所谓基于 MAC 的 VLAN，是指借助智能管理软件根据 MAC 地址来划分 VLAN。该划分方式一般用在每一交换机端口只连接一个终端的情况。也就是说，当端口级联傻瓜交换机时，

该种划分方式并不适用。端口借助网络包的 MAC 地址、逻辑地址或协议类型来确定其 VLAN 的从属，将端口划分至不同 VLAN。

基于 MAC 地址决定所属 VLAN 的，因此可以理解为这是一种在 OSI 的第二层设定访问链接的办法。当一网络节点刚连接到交换机时，此时交换机端口尚未分配，于是交换机通过读取网络节点的 MAC 地址，动态地将该端口划入某个虚拟网。一旦动态 VLAN 配置完成，用户的计算机就可以随意改变其连接的交换机端口，而不会由此而改变自己的 VLAN。当然，基于 MAC 地址的 VLAN，在设定时必须调查所连接的所有计算机的 MAC 地址并加以登录。而且如果计算机交换了网卡，就需要更改设定。当网络中出现未定义的 MAC 地址时，交换机可以按照预先设定的方式向网管人员报警，再由网管人员作相应的处理。

例如，网络管理员有一台笔记本电脑，由于工作性质的关系，需要经常到各部门联机工作。当该笔记本电脑从端口 A 移动到端口 B 时，交换机能够自动识别经过端口 B 的源 MAC 地址，自动把端口 A 从当前 VLAN 中删除，而把端口 B 定义到当前 VLAN 中（如图 2-6 所示）。这种定义方法的优点是当终端在交换式网络中移动时，不必重新定义虚拟网，交换机能够自动进行识别和定义。因此，基于 MAC 的 VLAN 也称为动态 VLAN。由于 MAC 地址具有唯一性，因此该 VLAN 划分方式的安全性也较高。

3. 基于 IP 的 VLAN

所谓基于 IP 的 VALN，是指根据 IP 地址来划分的 VLAN。交换机属于 OSI 的第二层，因此普通交换机不能识别帧中的网络层报文，但随着第三层交换机的出现，将第二层的交换功能和第三层的路由功能结合在一起，从而使交换机也能够识别网络层报文，可以使用报文中的 IP 地址来定义 VLAN。不像基于 MAC 地址的 VLAN，即使计算机因为交换了网卡或是其他原因导致 MAC 地址改变，只要它的 IP 地址不变，就仍可以加入原先设定的 VLAN。

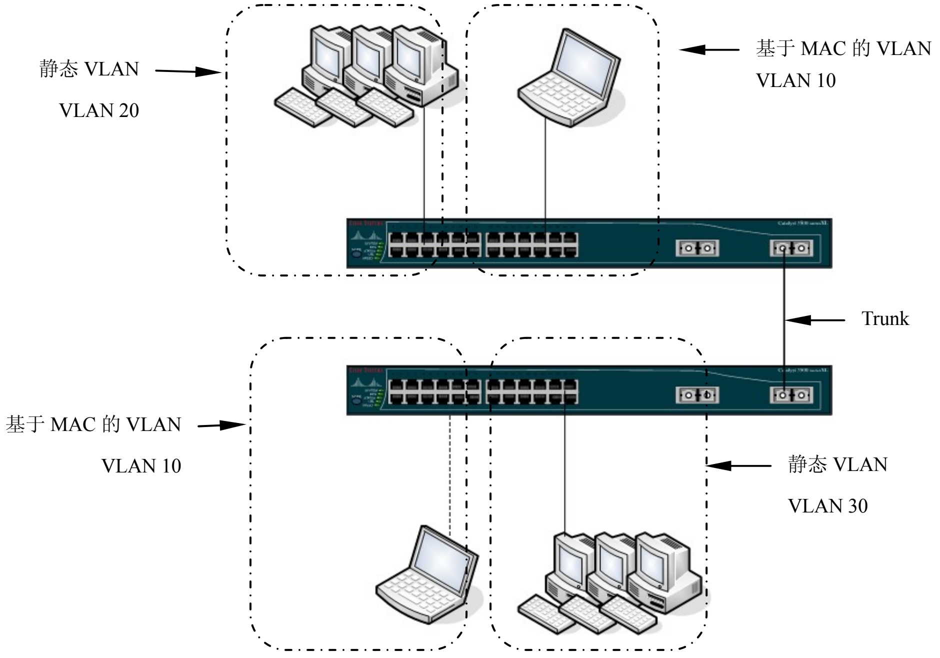


图 2-6　基于 MAC 地址的 VLAN

当某一用户设置有多个 IP 地址时，通过基于 IP 的 VLAN，该用户或该端口就可以同时访问多个虚拟网。在该模式下，位于不同 VLAN 的多个业务部门（每种业务设置成一个虚拟网）既可同时访问同一台网络服务器，也可以同时访问多个虚拟网的资源，还可让多个虚拟网间的连接只需一个路由设备完成。这种定义方法的优点是当某一终端使用的网络层协议或 IP 地址改变时，交换机能够自动识别，重新定义 VLAN，不需要网络管理员干预。但是，由于 IP 地址可以人为地、不受约束地自由设置，因此使用该方式划分 VLAN 也会带来安全上的隐患。

与基于 MAC 地址的 VLAN 相比，基于 IP 地址的 VLAN 能够更为简便地改变网络结构。IP 地址是 OSI 参照模型中第三层的信息，所以，可以理解为基于子网的 VLAN 是一种在 OSI 的第三层设定访问链接的方法。一般路由器与三层交换机都使用基于子网的方法划分 VLAN。

4. 基于用户的 VLAN

基于用户的 VLAN，则是根据交换机各端口所连的计算机上当前登录的用户，来决定该端口属于哪个 VLAN。这里的用户识别信息，一般是计算机操作系统登录的用户，比如可以是 Windows 域中使用的用户名。显然用户名信息，属于 OSI 第四层以上的信息。总的来说，决定端口所属 VLAN 时利用的信息在 OSI 中的层面越高，就越适于构建灵活多变的网络。

5. 基于组播的 VLAN

基于组播的 VLAN，就是动态地把那些需要同时通信的端口定义到一个 VLAN 中，并在 VLAN 中用广播的方法解决点对多点通信的问题。这种划分方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展。该 VLAN 划分方式主要适合于不在同一地理区域的局域网用户组成一个 VLAN，而不太适用于局域网，主要是效率不高。

2.2.3 VTP 技术

VTP 域（也称 VLAN 管理域）由一个或多个相互连接的、使用相同 VTP 域名的交换机组成。一台交换机能够被配置而且也只能被配置一个 VTP 域。使用命令行界面或 SNMP，可以修改全局 VLAN 的域配置。

1. VTP 简介

VTP 利用第 2 层中继帧，在一组交换机之间进行 VLAN 通信。VTP 从一个中心控制点开始，维护整个局域网络中 VLAN 的添加、添加和重命名工作，确保 VLAN 配置的一致性。有了 VTP，就可以在一台交换机集中进行 VLAN 配置变更，所作的变更会被自动传播到网络中所有其他的交换机上，当然，前提是这些交换机位于同一个 VTP 域。

■ VTP 工作原理

同一 VTP 域中的交换机共享它们的 VLAN 信息，并且一个交换机只能参加到一个 VTP 管理域，不同域中的交换机不能共享 VTP 信息。

交换机间交换下列信息：

- 管理域域名。

- 配置的修订号。交换机使用配置修正号，来决定当前交换机的内部数据是否应该接受从其他交换机发来的 VTP 更新信息。如果接收到的 VTP 更新配置修订号与内部数据库的修订号相同域者比它小，交换机忽略更新。否则，就更新内部数据库，接受更新信息。
- 已知虚拟局域网的配置信息。

VTP 的运行有如下特点：

- VTP 通过发送到特定 MAC 地址 01-00-0C-CC-CC-CC 的组播 VTP 消息进行工作。
- VTP 通告只通过中继端口传递。VTP 通告可以封装在 ISL 或者 IEEE802.1Q 帧内。
- VTP 消息通过 VLAN1 传送（这也是不能从中继链路中删除 VLAN1 的原因）。
- 经过 DTP 自动协商，启动中继之后，VTP 信息就可以沿着中继链路传送。
- VTP 域内的每台交换机都定期在每个中继端口上发送通告到保留的 VTP 组播地址。

■ **VTP 域**

VTP 域，也称为 VLAN 管理域，由一个以上共享 VTP 域名的相互连接的交换机组成。使用 VTP，必须为每台交换机指定 VTP 域名。VTP 信息只能在 VTP 域内保持。一台交换机可属于并且只属于一个 VTP 域。

默认状态下，交换机处于 VTP Server 模式，并且在收到由中继转发的 VTP 通告（VTP Advertisement）或配置至一个管理域之前，一直处于非管理域状态。在指定或学习管理域名前，不能在 VTP 服务器上建立或修改 VLAN。

如果交换机收到一个从中继连接传来的 VTP 通告，它将继承管理域名和 VTP 配置版本号，并且不再理睬不同的管理域名或更早的配置版本号。

如果将交换机配置为 VTP 透明模式，虽然可以建立可修改 VLAN，但是，修改将只影响被直接配置的交换机。

当修改位于 VTP Server 上的 VLAN 配置时，该修改将传播至 VTP 域中所有的交换机。VTP 通告被发送至所有的中继连接，包括 Inter-Switch Link（ISL）、IEEE 802.1Q、IEEE 802.10 和 ATM LAN Emulation（LANE）。

■ **VTP 模式**

可以将交换机配置在以下任何一种 VTP 模式下操作。

- Server

在 VTP Server（服务器）模式，可以为整个 VTP 域建立、修改和删除 VLAN，并指定其他配置参数（如 VTP 版本和 VTP 修剪）。VTP 服务器向其他在相同 VTP 域的交换机通告它们的 VLAN 配置，并同步它们的 VLAN 配置。VTP Server 是默认模式。

- Client

VTP Client（客户端）在许多行为上与 VTP Server 相同，不同之处在于只能被动接受 VLAN 配置信息，而不能在 VTP Client 上建立、修改或删除 VLAN。

- Transparent

VTP Transparent（透明）交换机不加入到 VTP。VTP Transparent 交换机不通告它的 VLAN 配置，并且不同步它的 VLAN 配置。然而，在 VTP 版本 2（VTP Version 2）中，Transparent 交换机向其中继端口转发它接收到的 VTP 通告。

■ **VTP 通告**

VTP 域中的每一台交换机都利用保留的多播地址，定期向其每一个中继端口发送通告。VTP 通告被相邻的交换机接收，并必然地更新它们的 VTP 和 VLAN 配置。

在 VTP 通告中，以下全局配置信息被分布，VLAN ID（ISL 和 802.1Q）、Emulated LAN 名（应用于 ATM LANE）、802.10 SAID 值（FDDI 网络）、VTP 域名、VTP 配置版本号、VLAN 配置（包括每个 VLAN 的 MTU 大小），以及帧格式。

■ **VTP 修剪**

VTP 修剪（VTP Pruning）通过减少不必要的泛洪（Flooded Traffic），如广播（Broadcast Packet）、多播（Multicast Packet）、未知（Unknown Packet）和泛洪（Flooded Unicast），从而提高网络带宽。

图 2-7 所示为未启用 VTP 修剪时的泛洪情况。

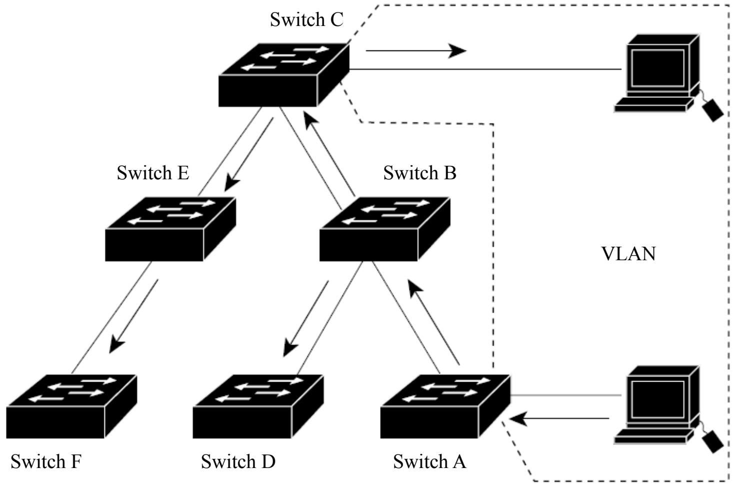


图 2-7　未启用 VTP 修剪

图 2-8 所示为启用 VTP 修剪后的泛洪情况。

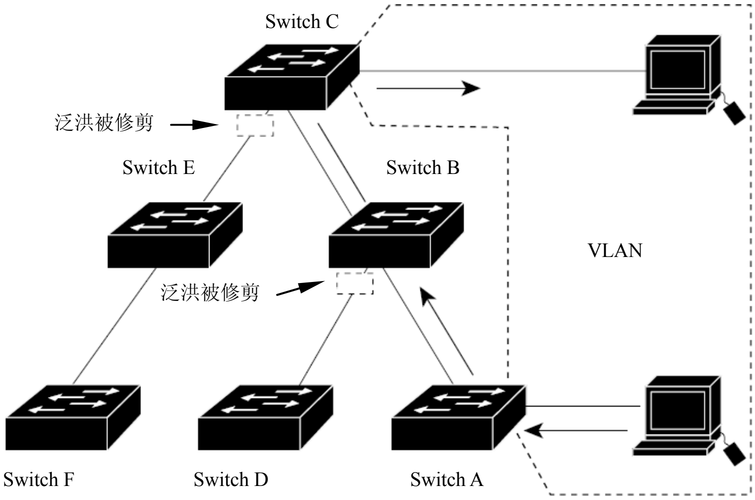


图 2-8　启用 VTP 修剪

VTP 修剪通过访问适当设备的方式，限制了到中继链接的泛洪，增加了网络的有效带宽。默认状态下，VTP 修剪未被启用。在启用 VTP 修剪之前，必须确认管理域中所有的设备都支持该功能。当在 VTP Server 上为整个管理域启用 VTP 修剪后，VTP 修剪将在几秒钟内实现。

2.2.4 私有虚拟网技术

通过私有虚拟网技术（Private Virtual Local Area Network，PVLAN）可以实现端口之间相互隔离，满足网络接入用户的安全性要求，避免用户信息和数据的泄露，防止非法攻击和窃取。在使用私有 VLAN 时，各接入端口间不可以相互通信，仅可通过上连端口访问网络资源。需要注意的是，第二层交换机和第三层交换机都可以创建 PVLAN。

1. VLAN 的局限性

随着局域网络应用的不断丰富，对网络数据通信的安全性将提出更高要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性。传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，每个用户被从第二层隔离开，可以防止任何恶意的行为和网络信息探听。然而，这种为每个客户分配单一 VLAN 和 IP 子网的模型造成了可扩展的局限。主要表现在以下几个方面。

- VLAN 的限制。交换机固有的 VLAN 总数支持的限制（例如，Cisco Catalyst 2960 最多支持 255 个 VLAN），导致局域网络不能划分太多数量的 VLAN，从而限制了网络应用。
- 复杂的 STP。对于每个 VLAN，每个相关的 Spanning Tree 的拓扑都需要管理，管理复杂繁琐。
- IP 地址的紧缺。IP 子网的大量划分势必造成大量 IP 地址的浪费，加之 IP 地址资源紧张，使 IP 地址的分配变得更加困难。
- 路由的限制。每个子网都需要相应的默认网关的配置，管理起来非常麻烦，而且增加了路由设备的负担，影响网络传输效率。

2. PVLAN 技术

同一 PVLAN 内连接到各端口的计算机彼此相互隔离，即使它们位于同一 IP 地址段，拥有相同的子网掩码和默认网关，也无法实现彼此之间的通信。若欲实现不同端口间的通信，只能经过默认网关，在第三层交换机中实现。

PVLAN 的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需与自己的默认网关连接，一个 PVLAN 不需要多个 VLAN 和 IP 子网就提供了具备第二层数据通信安全性的连接。所有用户都接入 PVLAN，从而实现了所有用户与默认网关的连接，而与 PVLAN 内的其他用户没有任何访问。PVLAN 功能可以保证同一个 VLAN 中的各个端口相互之间不能通信，但可以穿过 Trunk 端口。这样，即使同一 VLAN 中的用户，相互之间也不会受到广播的影响，如图 2-9 所示。

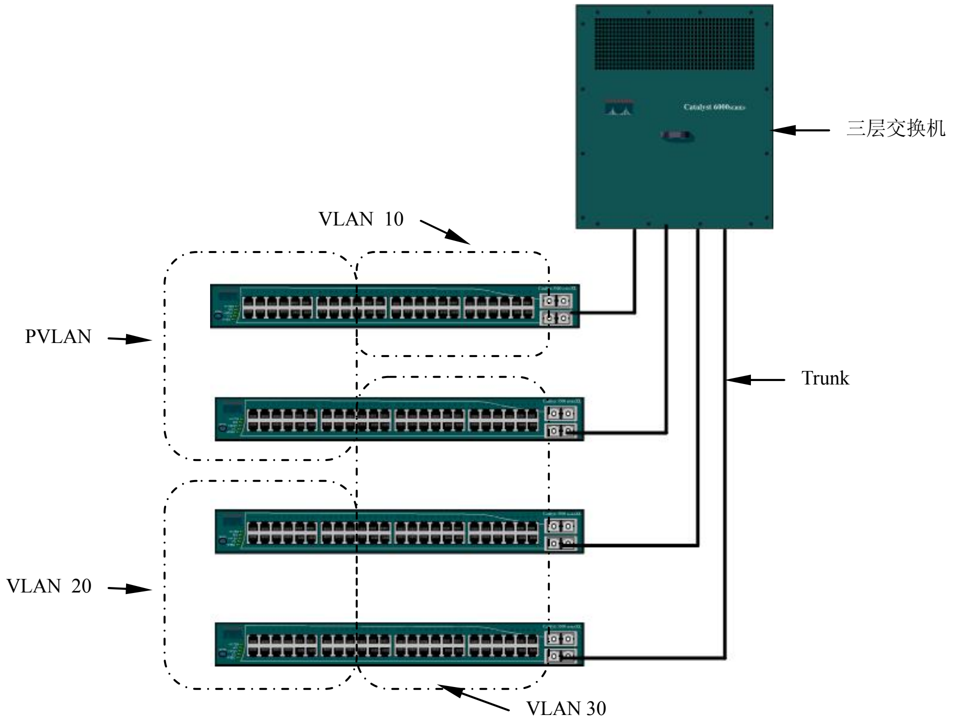


图 2-9　私有虚拟网技术

由此可见，PVLAN 技术在解决通信安全、防止广播风暴和浪费 IP 地址方面的优势是显而易见的，而且采用 PVLAN 技术有助于网络的优化。另外，PVLAN 的配置也相对简单，不必占用 VLAN 资源。

2.3　多层交换技术

交换机是典型的 OSI 二层设备，借助源和目的 MAC 地址实现端口间的快速转发。然而，随着虚拟网技术的推出，为了实现虚拟网络之间的快速路由转发，三层技术应运而生。而为了实现对各种网络服务的快速访问，四层技术也成为核心层交换机的必备。

2.3.1　第三层交换技术

在计算机数量众多的局域网络中，为了提高网络安全性和通信效率必须划分 VLAN，而不同 VLAN 间的通信只有通过路由设备才能实现。

如果使用传统路由器作为 VLAN 间的路由设备，将由于其吞吐量太小而很难适应大规模、高速率网络传输的需要，这无疑将成为千兆位以太网或万兆位以太网网络传输的瓶颈。于是，专门用于解决 VLAN 间通信的、集第三层转发与第二层交换于一身的第三层交换技术产生了。第三层交换机实际上是使用了集成电路的路由器，但比传统的路由器提供了更高的速度和更低的成本，也比传统的路由器更易于管理。正因为第三层交换机集成了路由器的功能，所以第三层交换机也被称为路由交换机（Routing Switch）。

由此可见，划分 VLAN 的网络必须使用三层交换机，否则 VLAN 之间将无法实现彼此之间的通信，如图 2-10 所示。

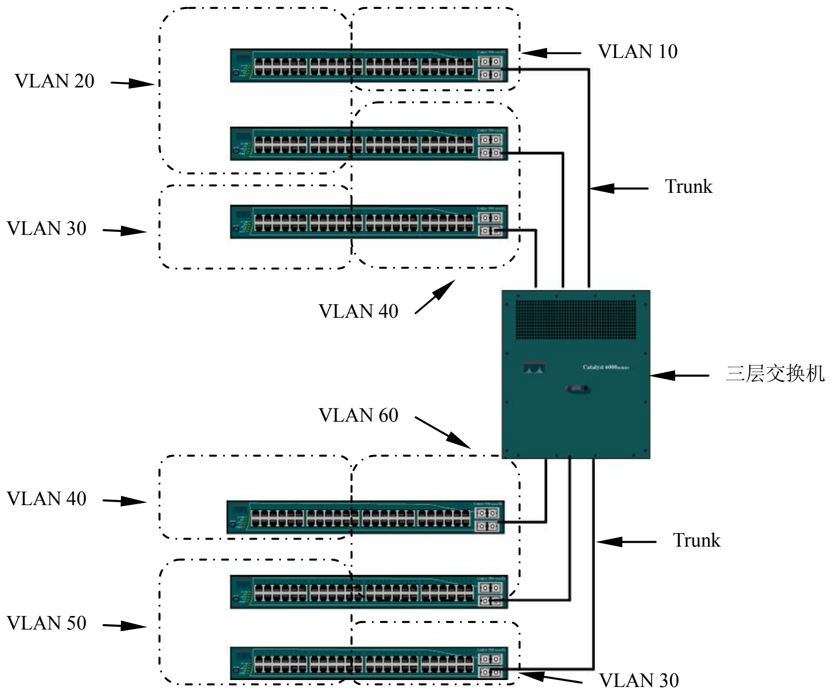


图 2-10　VLAN 间借助三层交换机通信

第三层交换机根据 OSI 参考模型网络层（即第三层）的 IP 地址完成端到端的数据交换，主要应用于不同 VLAN 子网间的路由。当某一信息源的第一个数据流进行第三层交换（路由）后，交换机会产生一个 MAC 地址与 IP 地址的映射表，并将该表存储起来，如同一信息源的后续数据流再次进入交换机，交换机将根据第一次产生并保存的地址映射表，直接从第二层由源地址传输到目的地址，不再经过第三层路由系统处理，提高了数据包的转发效率，解决了 VLAN 子网间传输信息时传统路由器产生的速率瓶颈。

第三层交换技术的强大功能表现在：

- 根据第三层协议对路由进行计算，其支持的路由协议包括 RIP（Routing Information Protocol，路由选择信息协议）和 OSPF（Open Shortest Path First，开放最短路径优先）等常用路由协议。
- 支持 IGMP（Internet Group Management Protocol，Internet 组管理协议）、DVMRP（Distance Vector Multicast Routing Protocol，距离矢量组播路由选择协议）等各种常用的 IP 组播协议，当交换式路由器收到组播报文后，首先将报文转发到包含组播组成员的 VLAN 上，继而再把报文转发到组播组成员的端口上。
- 支持服务质量（QoS），将报文赋予特定的优先级，不同优先级的报文送到不同的队列按先后转发。
- 支持标准的 SNMP（Simple Network Management Protocol，简单网络管理协议）协议，支持传统的命令行界面（Command Line Interface，CLI）。
- 对虚拟网的多种划分策略，尤其是它不仅支持传统的基于端口的 VLAN 划分，而且

还支持基于 IP 地址，子网号和协议类型的 VLAN 划分，这给园区网的管理带来极大的方便。

2.3.2 第四层交换技术

OSI 参考模型的第四层是传输层。传输层负责端到端通信，即在网络源和目标系统之间协调通信，是 IP 协议栈中 TCP（传输控制协议）和 UDP（用户数据报协议）所在的协议层。TCP 和 UDP 包含端口号，用于区分数据包所包含的应用协议（如 HTTP、FTP、E-mail 等）。第四层交换技术正是利用 TCP/UDP 端口号所提供的信息来区分包中的数据。

第四层交换技术不仅可以完成端到端交换，还能根据端口主机的应用特点，确定或限制其交换流量。简单地说，第四层交换技术是基于传输层数据包的交换过程的，是一类基于 TCP/IP 协议应用层的应用交换需求的新型局域网交换机，可以根据 TCP/UDP 端口号区分数据包的应用类型，从而实现应用层的访问控制和服务质量保证。通过查看第三层数据包头源地址和目的地址的信息，采取相应的动作，实现带宽分配、故障诊断和对 TCP/IP 应用程序数据流进行访问控制等功能。通过任务分配和负载均衡优化网络，提供详细的流量统计信息和记账信息等方式，在应用的层级上解决网络拥塞、网络安全和网络管理等问题，使网络具有智能和可管理等特性。

图 2-11 所示为四层交换机将不同的访问请求直接转发到提供相应服务的端口，从而实现对网络服务的高速访问。

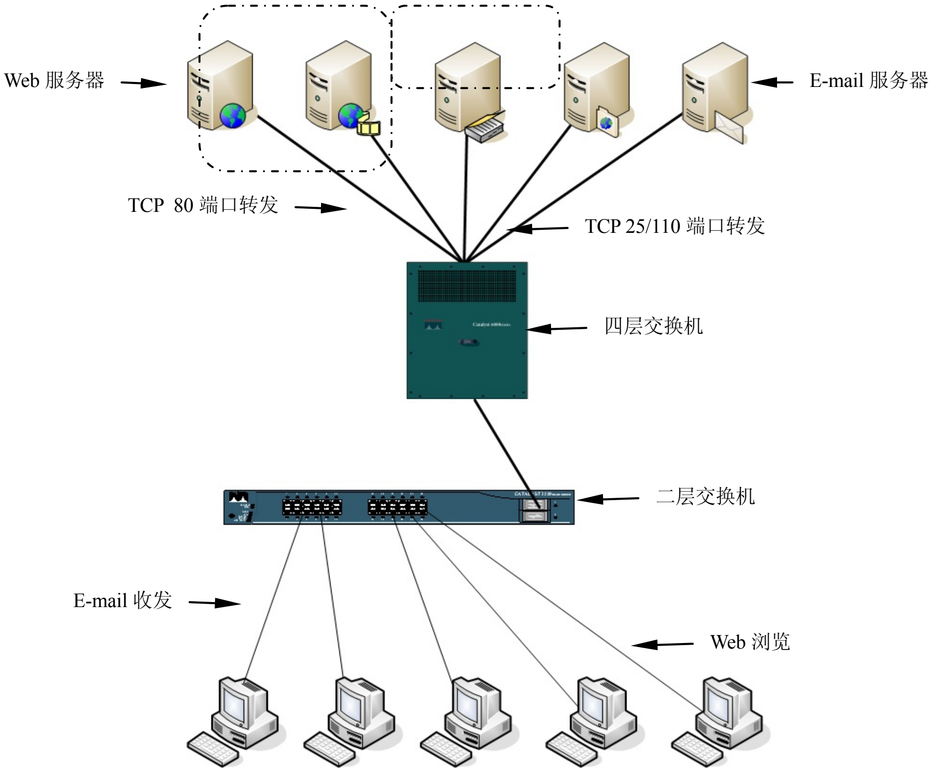


图 2-11 四层交换

第四层交换技术的主要功能如下：

- 数据包过滤。采用第四层信息端口号定义访问控制列表过滤规则，并借助 ASIC 专用高速芯片实现线速过滤控制。
- 服务质量。借助 TCP/UDP 第四层的端口号（即网络应用）信息区分优先级，设置优先级队列，确保重要的流量（如 VoIP、视频会议等对实时性要求较高的应用）得到最快的处理，使紧急应用获得网络的高级别服务。
- 负载均衡。按照 IP 地址和 TCP 端口进行虚拟连接的交换，直接将数据包发送到目的计算机的相应端口中，从而实现完美的服务器负载均衡。由于第四层交换基于硬件芯片，因此性能非常优秀。采用第四层交换机设备，所有的群集主机通过第四层交换机与外部网络相连，外部客户访问服务器时通过第四层交换机动态分配服务器，实现动态负载均衡，当其中一台服务器出现故障时，由交换机动态将所有流量分配到群集中的其他主机上。
- 主机备用连接。主机备用连接为端口设备提供了冗余连接，从而在交换机发生故障时有效保护系统，这种服务允许定义主交换机和备用交换机，同虚拟服务器定义一样，它们有相同的配置参数。由于第四层交换机共享相同的 MAC 地址，备份交换机接收和主单元全部一样的数据，使得备份交换机能够监视主交换机服务的通信内容。主交换机持续地通知备份交换机第四层数据、MAC 数据，以及电源状况。主交换机失败时，备份交换机就会自动接管，不会中断对话或连接。
- 统计与报告。通过查询第四层数据包，第四层交换机能够提供更详细的统计记录。因为管理员可以收集更详细的、哪个 IP 地址在进行通信的信息，甚至可根据通信中涉及到哪个应用层服务来收集通信信息。当服务器支持多个服务时，这些统计对于考察服务器上每个应用的负载尤其有效。增加的统计服务对于使用交换机的服务器负载均衡服务连接同样十分有用。

2.4 链路冗余技术

冗余是达成高可用性目的的根本手段。也就是说，若欲打造高可用性网络，那么，除了网络设备的冗余之外，链路冗余也是必不可少的。甚至可以说，没有链路冗余就不可能真正实现网络的高可用性。

2.4.1 扩展树技术

扩展树（Spanning Tree），也称生成树，它的产生源于链路的冗余连接。扩展树协议指通过一定算法，使任意两个节点间有且只有一条路径连接。这就好像是一棵树，从树根开始长起，然后是树干、树枝，最后到树叶，从而保证任意两片树叶间只有一条路径。

1. 扩展树的作用

在大中型的局域网络中，与中心交换机和服务器的连接非常重要，而端口或交换机却不可避免地存在着发生故障的可能性。那么，如何保证在一条链路发生故障之后，还能通过其他链路保持连接不被中断呢？这自然就要采用冗余链接（如图 2-12 所示）。然而，冗余的链接虽

然增加了系统的安全性，但同时也带来了另外一个问题，那就是链路循环（拓扑环），使得数据在交换机之间循环传递，并最终导致网络瘫痪。

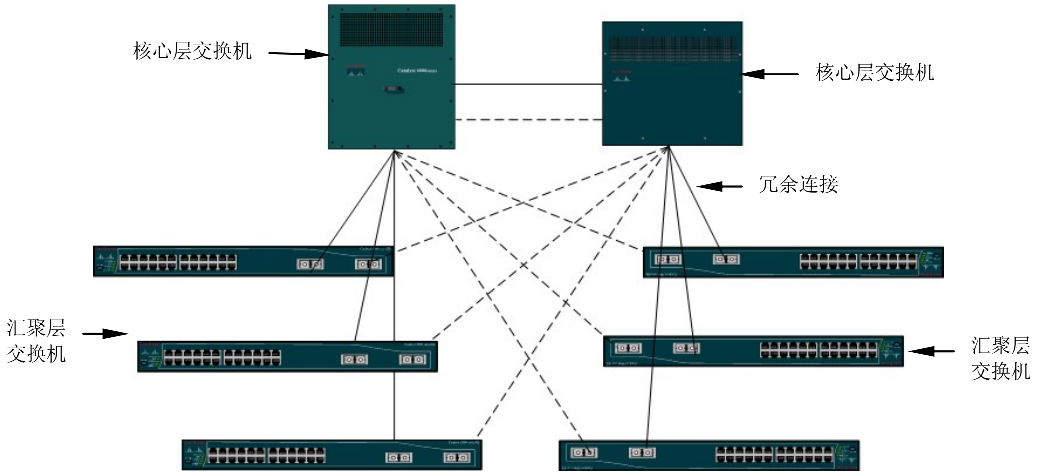


图 2-12　冗余链接

既然冗余备份是必需的，而又不能让两条以上的链路同时工作，那么唯一途径就是让两条链路中的一条处于工作状态，而另一条处于待命状态。处于待命状态的备份链路必须同时具有监视主链路工作状况的能力，并在主链路发生故障时，立即投入使用。这样既起到了备份的作用，又保证网络不会陷入死循环。于是，扩展树的思路诞生了。

另外，借助于扩展树技术，即使由于网络管理员的错误连接而导致了网络的拓扑环路，网络仍然可以正常运行，从而保证网络的连接稳定。

2.　STP

通过一定算法，STP 使任意两个节点间有且只有一条路径连接，而其他的冗余链路则被自动阻塞，作为备份链路。只有当活动链路失败时，备份链路才会被激活，从而恢复设备之间的连接，保证网络的畅通。

■　STP 简介

STP 协议是用来避免链路环路产生的广播风暴、并提供链路冗余备份的协议。

对二层以太网而言，交换机之间只能有一条活动着的通路，否则就会产生广播风暴。但是，为了提高局域网的可靠性，建立冗余链路又是必要的，其中的一些链路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作，使交换机起到以下作用。

- 发现并启动局域网的一个最佳树型拓朴结构。
- 发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择了可能的最佳树型结构。

这就好像是一棵树，从树根开始长起，然后是树干、树枝，最后到树叶，从而保证任意两片树叶间只有一条路（如图 2-13 所示）。而链路选举的标准就是优先级值（Priority）和端口

开销（Cost）。不过，Spanning-Tree 的优点是可以在任何端口实现，而不一定是固定的双绞线端口或光纤端口。

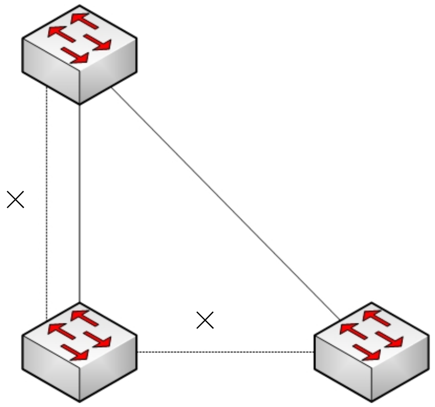


图 2-13　Spanning-Tree

注：虚线链路表示备份线路。

> **提示**
> 与 EtherChannel 不同，STP 只能保证在两台设备间拥有一条活动链路，因此，也就无法实现带宽加倍和负载均衡。

■　**STP 算法**

IEEE 802.1D 标准定义了 STP 的生成树算法。该算法依赖于 BID、路径开销和端口 ID 参数来做出决定。

●　BID（网桥 ID）

决定了桥接网络的中心，称为根网桥或根交换机。BID 参数是一个 8 字节域，前 2 个字节（十进制数）称为“网桥优先级”，后 6 个字节（十六进制数）是交换机的一个 MAC 地址。网桥优先级小的 BID 优先，当网桥优先级相同时，BID 中的后 6 个字节的 MAC 小的则 BID 优先。

●　路径开销

决定到根网桥（根交换机）的路径。路径开销是用来衡量网桥之间的距离的远近的，路径开销与跳数无关，其值是两个网桥之间某条路径上所有链路开销的总和。最小的路径开销是到根交换机的最佳路径。带宽越大，STP 开销越小。

●　端口 ID

也决定到根交换机的路径。由 2 个字节组成，包括“端口优先级”和“端口号”，各占 8 位。端口 ID 大小的判定与 BID 相同。

STP 通过发送 BPDU（Bridge Protocol Data Unit，网桥协议数据单元）传递生成树协议，并执行判别过程，以生成无拓扑环的网络拓扑。BPDU 是网桥之间用来交换生成树信息的特殊帧，包括根 BID、根路径开销、发送者 BID 和端口 ID 信息。BPDU 在网桥之间传播，包括交换机和所有配置来进行桥接的路由器。

判别过程如下：

（1） 确定根交换机。

（2） 计算到根交换机的最小路径开销。

（3） 确定最小的发送者 BID。

（4） 确定最小的端口 ID。

网桥为每个端口存储一个其收到的最佳 BPDU，当有其他 BPDU 到达交换机的端口时，将依据上述顺序判断此 BPDU 是否比原来存储的 BPDU 更好。如果新收到的 BPDU（或者本地生成的 BPDU）更好，则替换原有值。

当一个网桥第一次被激活时，其上所有端口每隔一个 HELLO 时间（默认 2 s）发送一次 BPDU；如果一个端口发现从其他网桥收到的 BPDU 比自己发送的好，则本地端口就停止发送 BPDU；如果在最大老化时间（默认 20 s）内没有从邻居网桥收到更好的 BPDU，则本地端口重新开始发送 BPDU，即最大老化时间是最佳 BPDU 的超时时间。

■ **STP 过程**

在网络第一次“初始化”时，所有网桥都泛洪 BPDU 信息，网桥通过执行判别过程，形成整个网络或 VLAN 唯一的生成树。在网络稳定后，BPDU 从根网桥流出，沿着无环支路到达网络中的每一个网段。当网络发生变化时，生成树协议按照上述收敛步骤重新作出处理。

生成树算法收敛于一个无环拓扑的初始过程，包含 3 个选举步骤。

（1） 选举一个根交换机。根交换机是一个具有最小 BID 的网桥，它是唯一的，是通过交换 BPDU 选举得出来的。也就是说，交换机通过传递 BPDU 来发现谁是最小的 BID，从而将具有最小 BID 的网桥作为根交换机。最初时，交换机总将自己认为是根网桥，当它发现有比自己小的 BID 时，就将收到的具有最小 BID 的交换机作为根网桥。

（2） 选举根端口。在根交换机选举完后，就开始选举根端口了。所谓根端口，就是按照路径开销最靠近根交换机的端口，也就是说具有最小根路径开销的端口。每一个非根交换机都必须选举一个根端口。

（3） 选举指定端口。此时，生成树算法还没有消除任何环路，因为还没有选举指定端口。所谓指定端口，就是连接在某个网段上的一个桥接端口，它通过该网段既向根交换机发送流量也从根交换机接收流量。桥接网络中的每个网段都必须有一个指定端口。指定端口也是根据最小根路径开销来决定的，因此根交换机上的每个活动端口都是指定端口，因为它的每个端口都具有最小根路径开销（实际上它的根路径开销是 0）。

> **提·示** 指定端口只在中继端口（TRUNK 口）起作用。接入端口在指定端口选举中不起任何作用。接入端口是用来连接到主机或者三层端口的。

■ **STP 端口状态**

每个启用扩展树的交换机二层接口，都将处于以下几种状态之一。

- 阻塞（Blocking）——处于阻塞状态的接口不参与帧的转发。初始化之后，BPDU 被发送至每个交换机接口。也就是说，阻塞状态接口不能接收或者转发数据，不能把 MAC 地址加入地址表，只能接收 BPDU 包。交换机作为根初始化，直至与其他交换机交换 BPDU。该交换用于确定网络中哪台交换机是根或作为根交换机。如果网络中

只有一台交换机，没有交换发生，转发延时计时器，接口将进入到侦听状态。交换机初始化之后，接口经常进入阻塞状态。或者说，处于学习、侦听或转发状态的端口，一旦检测到有桥接环，或者失去其根端口或指定端口的状态，将返回至阻塞状态。

- 侦听（Listening）——当扩展树决定该接口参与帧转发时，侦听状态为阻塞状态之后的第一个过渡状态。如果一个端口可以成为一个根端口或指定端口，即可进入侦听状态。此时接口不能接收或者转发数据，也不能将 MAC 地址加入地址表，但是，可以接收和发送 BPDU 包。
- 学习（Learning）——该端口准备参与帧转发。在转发延迟时间后（默认 15 s），端口进入学习状态。此时，该端口不能转发数据，但是，可以发送和接收 BPDU 包，也可以学习 MAC 地址，并将其加入地址表。
- 转发（Forwarding）——该端口转发帧。此时端口能够发送和接收数据，学习 MAC 地址并添加至地址表，也可以接收和发送 BPDU 包。
- 禁用（Disabled）——该端口没有参与扩展树，因为该端口处于关闭（shutdown）、未连接状态，或者该端口没有扩展树实例。为了管理或者因为发生故障将端口关闭。

接口状态变化过程如下（如图 2-14 所示）。

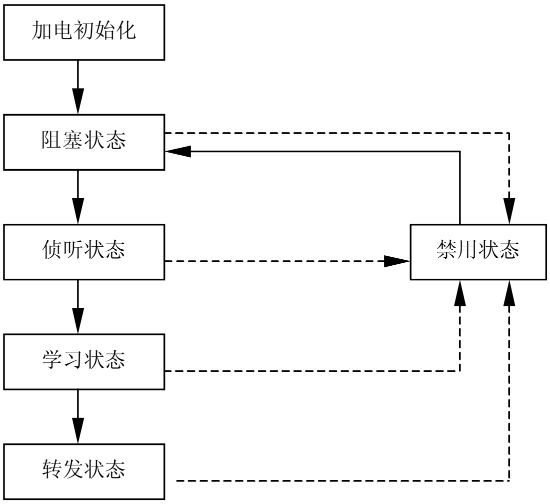


图 2-14　扩展树接口状态变化过程

- 从初始化到阻塞。
- 从阻塞到侦听或禁用。
- 从侦听到学习或禁用。
- 从学习到转发或禁用。
- 从转发到禁用。

■ STP 缺点

STP 虽然能够解决拓扑环路的问题，不过，仍然存在以下缺陷。

- 由于整个交换网络只有一个生成树，在网络规模比较大的时候会导致较长的收敛时间，拓扑改变的影响面也较大。

- IEEE 802.1Q 逐渐成为交换机的标准协议。在网络结构对称的情况下，单生成树没有什么问题。但是，在网络结构不对称时，单生成树就会影响网络的连通性。

3. RSTP

RSTP（Rapid Spaning Tree Protocol，快速生成树协议）通过快速生成树算法在交换网络中阻断部分冗余路径，建立起无环路的树状网络。RSTP 执行的 802.1w 协议，由 STP 的 802.1d 协议发展而来。RSTP 协议完全向下兼容 802.1D STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快”。如果一个局域网内的网桥都支持 RSTP 协议且配置得当，一旦网络拓扑改变而要重新生成拓扑树只需要不超过 1 s 的时间（传统的 STP 大约需要 50 s）。对于像语音和视频这些对延迟敏感的网络应用至关重要。

RSTP 针对各种端口在拓扑结构中角色的不同，对某些端口实现了从阻塞状态到转发状态的瞬间迁移或快速迁移。因此，RSTP 协议在网络结构发生变化时，能更快地收敛网络。RSTP 利用点到点线路并提供生成树的快速收敛。

RSTP 根据端口在活动拓扑中的作用，定义了 5 种端口角色。

- Disabled（非活动端口）——不参与 RSTP 的运算。
- Root（根端口）——其所在网桥连接到根网桥，并且网桥通过根端口到达根网桥的路径代价最低。
- Designated（指定端口）——通过其所在网桥将连接在其上的一个局域网连接到根网桥。
- Alternate（替代端口）——提供网桥到根网桥除了根端口到根网桥的路径外的替代路径。
- Backup（备份端口）——为处在网桥下游的（远离树根方向的）局域网提供到根网桥的替代路径。

其中，根端口和指定端口是活动拓扑的一部分，它们进行地址学习并且正常地转发数据。替代端口、备份端口和非活动端口则不是活动拓扑的组成部分，它们不进行地址学习和数据转发。

> **提·示** RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号来自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 网桥互连就只能按 STP 的转发方法，过 30 s 再转发，无法发挥 RSTP 的最大功效。

4. PVST/PVST+

PVST（Per-VLAN Spanning Tree，每 VLAN 生成树）是在 VLAN 上处理生成树的 Cisco 特有解决方案。PVST 为每个虚拟局域网运行单独的生成树实例。通常情况下，PVST 要求在交换机之间的中继链路（Trunk）上采用 Cisco ISL 协议。

PVST＋协议对 PVST 协议进行了改进，并成为交换机默认的生成树协议。PVST＋协议在 VLAN 1 上运行的是普通 STP 协议，在其他 VLAN 上运行 PVST 协议。

由于每个 VLAN 都有一棵独立的生成树，因此，单生成树的主要缺陷基本上都被解决了。

同时，PVST 还能够支持二层的负载均衡。

当然，PVST/PVST+也有如下缺陷。

- 由于每个 VLAN 都需要生成一棵树，PVST BPDU 的通信量将正比于 Trunk 的 VLAN 个数。
- 在 VLAN 个数比较多的时候，维护多个生成树的计算量和资源占用量将急剧增长。特别是当 Trunk 了很多 VLAN 的接口状态变化的时候，所有生成树的状态都要重新计算，CPU 将不堪重负。所以，Cisco 交换机限制了 VLAN 的使用个数，同时不建议在一个端口上 Trunk 很多 VLAN。
- 由于协议的私有性，PVST/PVST＋不能像 STP/RSTP 一样得到广泛的支持，不同厂家的设备并不能在这种模式下直接互通，只能通过一些变通的方式实现。

一般情况下，网络的拓扑结构不会频繁变化，所以，PVST/PVST＋的这些缺点并不会很致命。但是，端口 Trunk 大量 VLAN 这种需求还是存在的。

5. MSTP

多生成树协议 MSTP（Multiple Spanning Tree Protocol）是 IEEE 802.1s 中定义的一种新型生成树协议。MSTP 与 STP/RSTP 一脉相承，三者有很好的兼容性。MSTP 是在传统的 STP、RSTP 的基础上发展而来的新的生成树协议，使用 RSTP 进行快速收敛。

由于传统的生成树协议与 VLAN 没有任何联系，因此，在特定网络拓扑下就会产生一些问题。MSTP 可以把一组 VLAN 划分为一个生成树实例（instance），有着相同实例配置的交换机就组成一个 MST 域（region），运行独立的生成树（该内部生成树称为 IST，Internal Spanning-Tree）。MST 域组合就相当于一个大的交换机，与其他 MST 域再进行生成树算法运算，得出一个整体的生成树，称为 CST（Common Spanning Tree，共同生成树）。

简单地说，STP/RSTP 是基于端口的，PVST＋是基于 VLAN 的，而 MSTP 是基于实例的。与 STP/RSTP 和 PVST+相比，MSTP 中引入了“实例”（Instance）和“域”（Region）的概念。所谓“实例”就是多个 VLAN 的一个集合，这种通过多个 VLAN 捆绑到一个实例中去的方法可以节省通信开销和资源占用率。MSTP 各个实例拓扑的计算是独立的，在这些实例上就可以实现负载均衡。使用时，可以把多个相同拓扑结构的 VLAN 映射到某一个实例中，这些 VLAN 在端口上的转发状态将取决于对应实例在 MSTP 里的转发状态。

> **提示** 与 STP 和 RSTP 相比，MSTP 具有 VLAN 认知能力，可以实现负载均衡，实现类似RSTP的端口状态快速切换;与PVST+相比,MSTP可以捆绑多个VLAN到一个实例中以降低资源占用率，并且可以很好地向下兼容 STP/RSTP 协议。

如图 2-15 所示，交换机 A 和 B 都在 MSTP 域 1 内，MSTP 域 1 没有环路产生，所以，没有链路被禁用。同理，MSTP 域 2 的情况也一样。然后，域 1 和域 2 就分别相当于两个大的交换机，这两台“交换机”间有环路，因此，根据相关配置选择一条链路被禁用。这样，既避免了环路的产生，也能让相同 VLAN 间的通信不受影响。

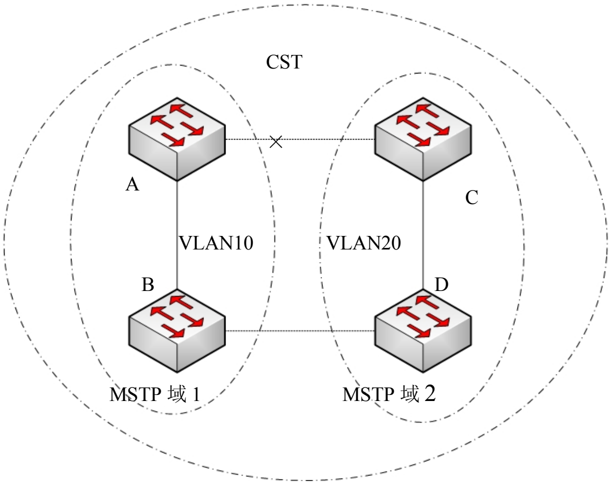


图 2-15 MSTP

PVST+、MSTP 和 Rapid-PVST+之间的协同性与兼容性如表 2-1 所示。

表 2-1 PVST+、MSTP 和 Rapid-PVST+之间的协同性与兼容性

	PVST+	MSTP	Rapid PVST+
PVST+	是	是（有限制）	是（PVST+有限制）
MSTP	是（有限制）	是	是（PVST+有限制）
Rapid PVST+	是（PVST+有限制）	是（PVST+有限制）	是

2.4.2 链路汇聚技术

链路汇聚（Multi Link Trunk，MLT）是指将多个交换机之间、交换机和路由器之间，以及交换机和服务器之间的并行链路同时使用，以增加设备间带宽的技术（如图 2-16 所示）。锐捷称之为 AP（Aggregate Port），Cisco 称之为链路汇聚（EnterChannel）。

1. 链路汇聚的作用

使用端口聚合协议（Port Aggregation Protocol，PAgP）或链路汇聚控制协议（Link Aggregation Control Protocol，LACP）可以将交换机之间、交换机和路由器之间，以及交换机和服务器之间的多条链路绑定在一起，叠加其传输带宽，使网络设备之间通信更加快速而顺畅，从而使快速以太网（Fast Ethernet）、千兆位以太网（Gigabit Ethernet）和万兆位以太网（10 Gigabit Ethernet）分别实现最高 400 Mbps、4 Gbps 和 40 Gbps 的连接带宽。

EtherChannel 的作用有以下几点。

■ **扩展网络带宽**

对于 10/100 Mbps 端口而言，Fast EtherChannel（FEC）无疑是一种廉价的千兆位以太网解决方案；对于 1000 Mbps 端口而言，Gigabit EtherChannel（GEC）则成倍地增加了网络带宽，消除了交换机之间由于级联而产生的瓶颈，满足交换机之间以及交换机与服务器之间的大量数据交换；对于 10 Gbps 端口而言，10 Gigabit EtherChannel 提供了无与伦比的网络带宽，完全

可以实现任何网络应用的无阻塞传输。

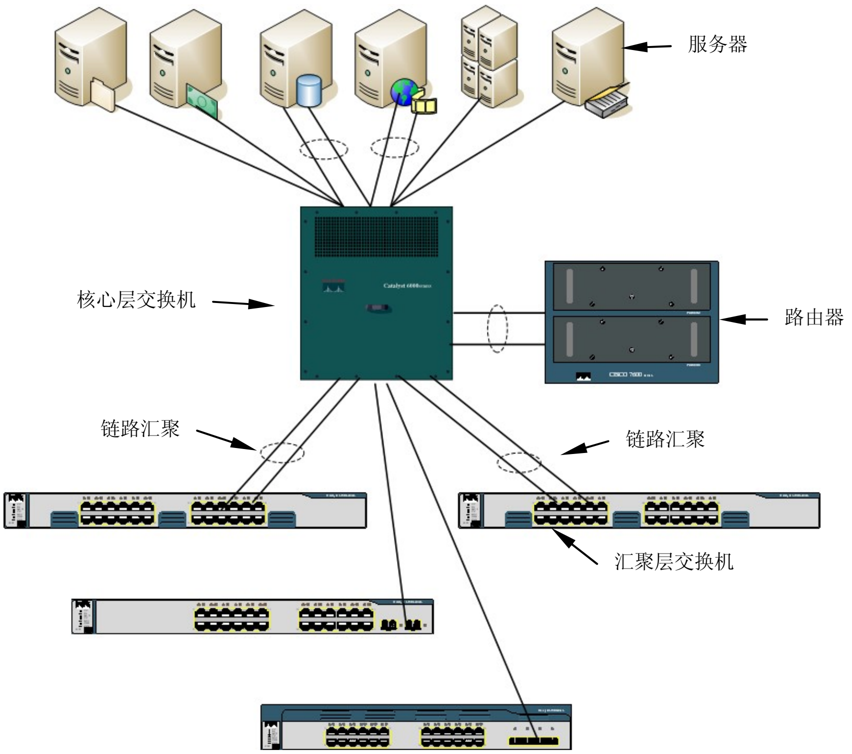


图 2-16　链路汇聚

■ **负载分担均衡**

所谓负载分担，是指当交换机之间或交换机与服务器之间在进行通信时，端口聚合的所有链路将同时参与数据的传输，从而使所有的传输任务都能在极短的时间内完成。线路占用的时间更短，网络传输的效率更高。同时，还可以根据网络传输的具体需求设置负载均衡的方式（包括源/目的端口、源/目的 IP 地址、源/目的 MAC 地址）。

■ **线路冗余备份**

所谓线路备份，是指当聚合链路的部分端口或连接出现故障时，并不会导致聚合链路连接的中断，非故障链路能够不受影响地正常工作，并承担所有失败链路的通信，从而增强了网络的稳定性和安全性。当然，此时的传输带宽将下降为保持正常的链路的带宽总和。

2. 链路汇聚协议

使用 PAgP 或 LACP 协议，可以很容易地在有 EtherChannel 能力的端口间，自动建立 Fast EtherChannel 和 Gigabit EtherChannel 连接，进行信息的交流。该协议具有学习相邻端口组动态和信息的能力。PAgP 是 EtherChannel 的增强版，支持在 EtherChannel 上的 Spanning Tree 和 Uplink Fast 功能，并支持自动配置 EtherChannel 的捆绑。

■ **PAgP 协议**

PAgP 支持模式：

- auto，当侦测到 PAgP 设备时，将只启用 PAgP。将端口置于被动协商状态，可以对接

收到的 PAgP 作出响应，但是，不能主动发送 PAgP 包进行协商。

- desirable，无条件启用 PAgP。将端口置于主动协商状态，通过发送 PAgP 包，主动与其他接口进行协商。
- on，将接口强行指定至 Channel。只有两个 on 模式接口组连接时，EtherChannel 才可用。
- non-silent，如果交换机连接到有 PAgP 能力的伙伴，可以将端口配置为 non silent（非沉默）运行。如果没有为 auto 或 desirable 模式指定 non-silent 关键字，默认为 silent。沉默设置被用于连接到文件服务器或包分析仪。该设置允许 PAgP，将端口添加至 Channel 组，并使用端口进行传输。

采用 PAgP 协议时，以下几种模式可以构建 EtherChannel。

- 一个端口为 desirable 模式，另一个端口为 desirable 或 auto 模式。
- 一个端口为 auto 模式，另一个端口为 desirable 模式。

■ **LACP 协议**

LACP 支持模式：

- active，当侦测到 LACP 设备时，将只启用 LACP。激活端口的主动协商状态，通过发送 LACP 包，与其他端口进行主动协商。
- passive，当侦测到 LACP 设备时，将只启用 LACP。将端口置于被动协商状态，可以对接收到的 LACP 作出响应，但是，不能主动发送 LACP 包进行协商。

采用 LACP 协议时，以下几种模式可以构建 EtherChannel。

- 一个端口为 active 模式，另一个端口为 active 或 passive 模式。
- 一个端口为 passive 模式，另一个端口也为 passive 模式。

在 Catalyst 交换机之间创建 EtherChannel 时，建议的端口模式如表 2-2 所示。

表 2-2　Catalyst 交换机之间创建 EtherChannel 时的建议模式

Catalyst 平台之间推荐 EtherChannl 模式		相邻 Catalyst 交换机		
		6800/6500/6000, 4900/4500/4000	3850, 3750, 3650, 3560, 3550, 2970, 2960, 2955, 2950, 2940	Express 500
本地 Catalyst 交换机	6800/6500/6000, 4900/4500/4000	本地 desirable，相邻 desirable	本地 desirable，相邻 desirable	本地 on，相邻 Static
	3850, 3750, 3650, 3560, 3550, 2970, 2960, 2955, 2950, 2940	本地 desirable，相邻 desirable	本地 desirable，相邻 desirable	本地 on，相邻 Static
	Express 500	本地 Static，相邻 on	本地 Static，相邻 on	本地 Static，相邻 Static

注意　不是所有型号的 Cisco Catalyst 交换机和所有的 Cisco IOS 版本都同时支持 PAgP 和 LACP 协议。因此，在配置链路汇聚前，应先查阅相关的技术文档，并采用双方都支持的链路汇聚协议，以避免配置失败。

2.4.3 路由冗余

中心交换机是整个网络的核心和心脏，如果发生致命性的故障，将导致本地网络的瘫痪，所造成的损失也是难以估计的。因此，对三层路由采用热备份是提高网络可靠性的必然选择。

利用 HSRP、VRRP、GLBP 协议保证核心设备的负荷分担和热备份，在中心交换机和双汇聚层交换机中的某台交换机出现故障时，三层路由设备和虚拟网关能够快速切换，实现双线路的冗余备份，保证整网稳定性。

1. 热备份路由器协议

热备份路由器协议（Hot Standby Router Protocol，HSRP）的设计目标是支持 IP 流量失败转移时不会引起混乱，并允许主机使用单路由器，以及即使实际第一跳路由器失败，也能保证路由器间的连通性。换句话说，当源主机不能动态了解第一跳路由器的 IP 地址时，HSRP 协议能够保护第一跳路由器不出故障。在 HSRP 协议中，多种路由器只对应一个虚拟路由器，即只支持一个路由器代表虚拟路由器实现数据包转发过程。终端主机将它们各自的数据包转发到该虚拟路由器上。

负责转发数据包的路由器称之为活动路由器（Active Router）。一旦活动路由器出现故障，HSRP 将激活备份路由器（Standby Routers）取代活动路由器（如图 2-17 所示）。HSRP 协议提供了一种决定使用活动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的默认网关地址。如果活动路由器出现故障，备份路由器承接活动路由器的所有任务，并且不会导致主机连通中断现象。

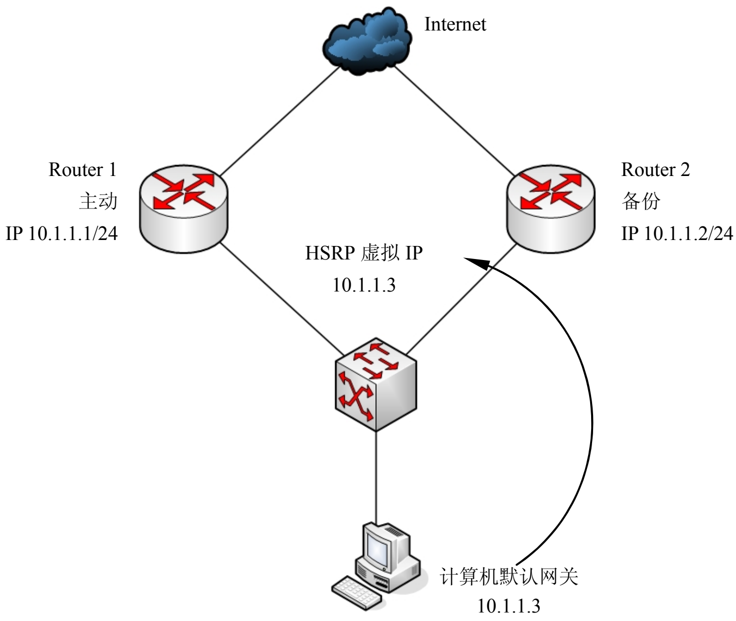


图 2-17　HSRP

提示　HSRP 运行在 UDP 上，采用端口号 1985。路由器使用它们的实际 IP 地址（而不是其虚拟 IP 地址）转发协议数据包，因此，HSRP 路由器间能相互识别，并在活动路由器故障时切换到备份路由器。

2. 多组热备用路由器协议

MHSRP（Multigroup Hot Standby Router Protocol，多组热备用路由器协议）是HSRP协议的扩展，它允许路由器的一个端口隶属于多个热备份组。MHSRP协议需要Cisco IOS 10.3或以上的版本支持，并且路由器硬件允许一个以太网端口绑定多个单点广播MAC地址。这些特殊路由器硬件允许配置路由器中的一个端口，使得该路由器成为多个备份组的备份路由器。

在某个局域网中，多个热备组可以共存和重叠。每个备份组都仿效一个虚拟路由器。对于每个备份组来说都有一个为别人所知的MAC地址，以及一个IP地址。而该IP地址应该是这个局域网中第一个子网中的地址，但必须不同于设置在所有路由器端口上的地址和局域网中主机的地址，甚至包括为其他HSRP组设的地址。

如图2-18所示，一半客户端配置使用路由器A作为默认网关，另一半客户端被配置使用路由器B作为默认网关，路由器A和路由器B建立两个HSRP组。对于1组而言，路由器A是默认活动路由器，因为它被赋予最高优先权，路由器A是备用路由器。在正常运行时，两个路由共同承担IP传输负载。当一个路由器发生故障时，另外一个路由器将承担整个网络的路由转发任务。

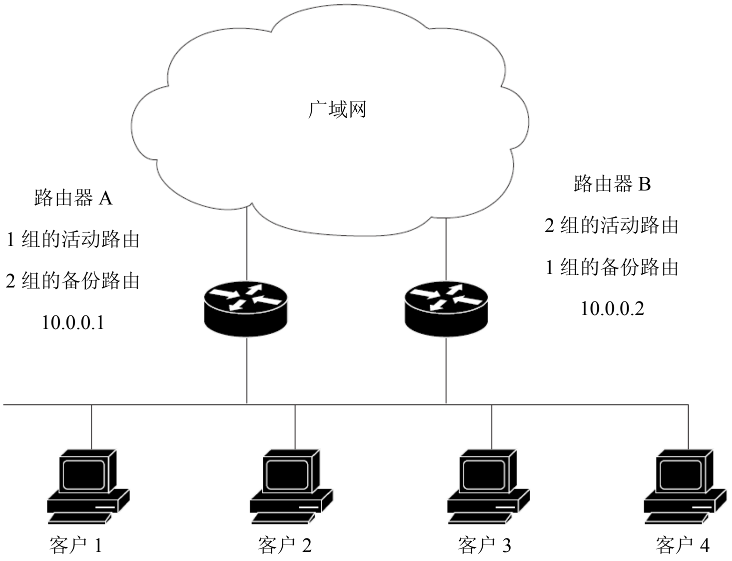


图2-18 MHSRP

3. 虚拟路由冗余协议

在网络中，一般给终端设备指定一个或多个默认网关（Default Gateway）。如果作为默认网关的三层设备损坏，那么所有使用该网关的主机通信必然中断。即使配置了多个默认网关，如不重新启动终端设备，也不能切换到新的网关。采用虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP）可以很好地避免静态指定网关的缺陷。

一组VRRP路由器协同工作，共同构成一台虚拟路由器，如图2-19所示。该虚拟路由器对外表现为一个具有唯一固定IP地址和MAC地址的逻辑路由器。同一VRRP组的路由器有

两种角色，即主控路由器和备份路由器。一个 VRRP 组中有且只有一台主控路由器，同时，可以有一台或多台备份路由器。VRRP 协议使用选择策略选出一台作为主控路由器，负责 ARP 响应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器，由于切换迅速且无需改变 IP 地址和 MAC 地址，所以对网络用户而言一切都是透明的。

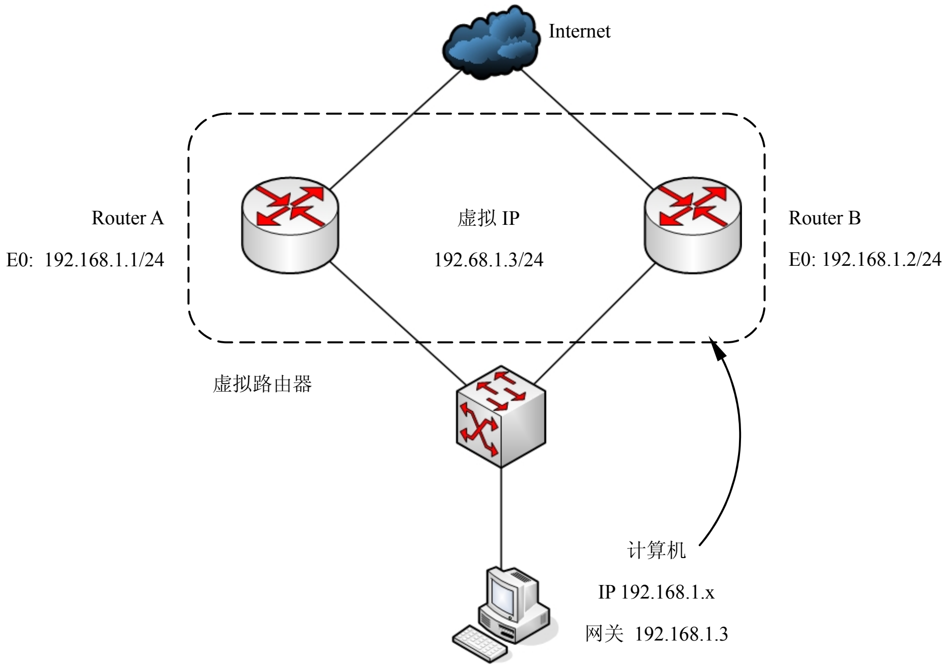


图 2-19　VRRP

4.　网关负载均衡协议

网关负载均衡协议（Gateway Load Balancing Protocol，GLBP）不仅提供冗余网关，还在各网关之间提供负载均衡，而 HRSP、VRRP 都必须选定一个活动路由器，备用路由器则处于闲置状态。

GLBP 可以绑定多个 MAC 地址到虚拟 IP，从而允许客户端选择不同的路由器作为其默认网关，而网关地址仍使用相同的虚拟 IP，从而实现一定的连接冗余。

优先级最高的路由器成为活动路由器（Active Virtual Gateway，AVG），其他非 AVG 提供冗余。某路由器被推举为 AVG 后，和 HRSP 不同的工作开始了，AVG 分配虚拟的 MAC 地址给其他 GLBP 组成员。所有的 GLBP 组中的路由器都转发包，但是各路由器只负责转发与自己的虚拟 MAC 地址相关的数据包，如图 2-20 所示。

每个 GLBP 组中最多有 4 个虚拟 MAC 地址，非 AVG 路由器由 AVG 按序分配虚拟 MAC 地址，非 AVG 也被称作活动虚拟发送者（Active Virtual Forwarder，AVF）。

AVF 分为两类，即主虚拟发送者（Primary Virtual Forwarder，PVF）和次虚拟发送者（Secondary Virtual Forwarder，SVF）。直接由 AVG 分配虚拟 MAC 地址的路由器被称作 PVF，后续不知道 AVG 真实 IP 地址的组成员，只能使用 hello 包来识别其身份，然后被分配虚拟 MAC 地址，此类路由器被称作 SVF。

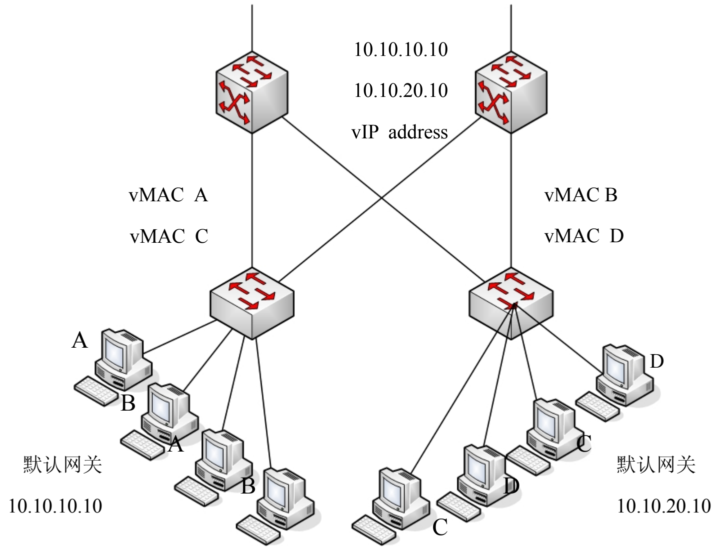


图 2-20　GLBP

当 AVG 失效时，推举过程就会发生，以决定哪个 AVF 替代 AVG 分配 MAC 地址。推举机制依赖于优先级。最多可以配置 1024 个 GLBP 组，不同的用户组可以配置成使用不同的组 AVG 作为其网关，以实现负载均衡。

2.5　VoIP 技术

IP 语音技术（Voice Over IP，VoIP），又称为 IP 电话或 IP 网络电话。IP 语音技术通过对语音信号进行编码数字化、压缩处理成压缩帧，然后转换为 IP 数据包在 IP 网络上进行传输，从而达到了在 IP 网络上进行语音通信的目的。

2.5.1　IP 语音技术

VoIP 可以在 IP 网络上廉价地传送语音、传真、视频和数据等业务，如统一消息、虚拟电话、虚拟语音/传真邮箱、查号业务、Internet 呼叫中心、Internet 呼叫管理、电视会议、电子商务、传真存储转发和各种信息的存储、转发等，甚至不必借助传统的语音电话链路。由于 Internet 就是一个最大的 IP 网络，因此 VoIP 最大的优势就是可以广泛地采用 Internet 和全球 IP 互连的环境，提供比传统业务更多、更好、更廉价的服务。图 2-21 所示为支持 VoIP 技术的交换机与 IP 电话。

图 2-21　支持 VoIP 技术的交换机与 IP 电话

不过，由于 IP 语音设备的价格较高，因此

往往很少单纯应用于局域网络，更多地被应用于远程网络间（如银行专用网络、税务专用网络、公安专用网络，公司总部与分支机构，尤其是跨地域甚至是跨国的大型公司）的实时通信（如图 2-22 所示）。

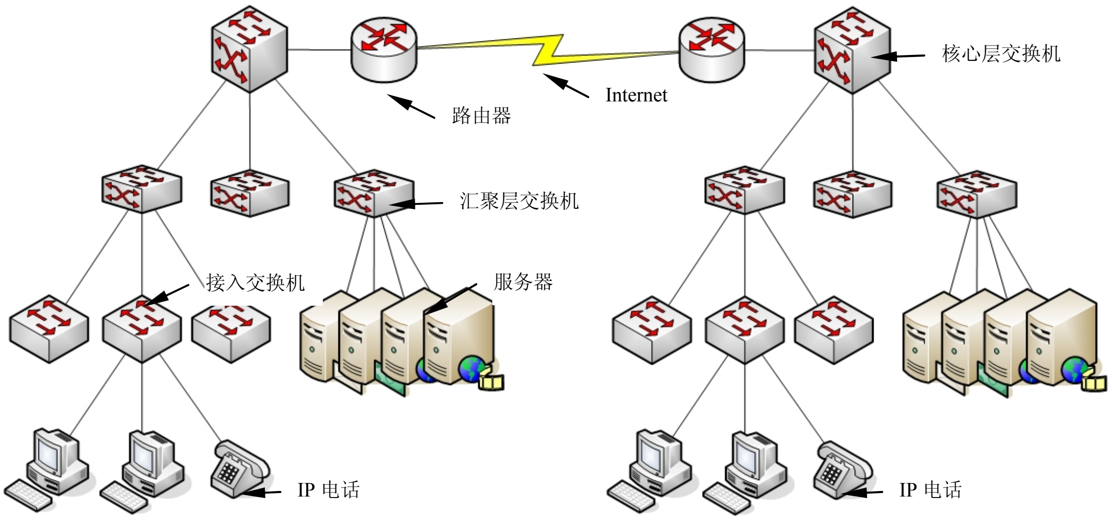


图 2-22　VoIP 技术

2.5.2 服务质量技术

通常情况下，在交换机中数据是按照先后顺序排队等待转发的，应用只能作为“尽力而为”业务（无保证的业务）传输，在网络传输量较大时，每个端口的数据都将在缓存中排队等待，并且当端口缓存被占用完毕时，还会将后续到达的数据直接丢弃。对于普通数据（如电子文档、程序文件等）而言，数据包先后到达的顺序并不重要，因为可以通过重组而得到恢复。但对于语音、视频等实时传输的数据而言，由于数据的先后顺序非常重要，因此在网络拥塞时话音和视频变得非常不稳定。可见，在网络带宽或设备处理能力有限的情况下，如果不采取相应的措施，交换机显然无法满足一些需要实时传输数据（IP 电话、电视会议及关键任务数据等）的需要。

服务质量（Quality of Service，QoS）技术可以觉察和测量出网络的性能，并可以指定各种网络应用的优先级别，从而使某些特殊应用（如视频会议、IP 电话等）享有优先转发权。当并发网络传输发生时，或者发生网络拥塞时，被指定网络应用总是能够优先被处理和转发，而普通网络应用的数据则将滞后传输甚至被丢弃。因此，借助于 QoS 技术，可以搭建完美的 VoIP 网络，有效地控制丢包率、延迟和抖动，解决网络延迟和阻塞等问题，从而实现完美的实时多媒体数据传输（如图 2-23 所示）。

由此可见，当各种网络应用较多、数据传输较为频繁时，若欲实现多媒体数据的完美传输，就必须采用 QoS 技术。

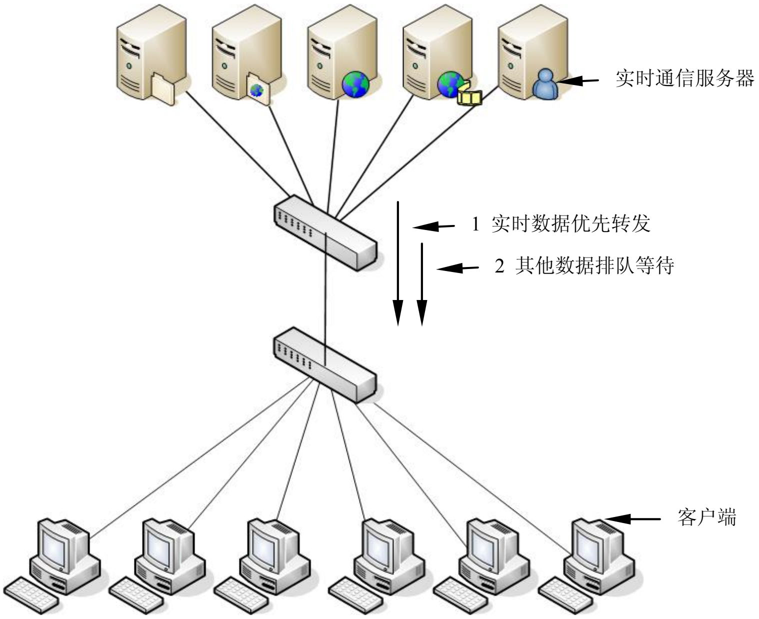


图 2-23　服务质量技术

2.6　安全技术

交换机作为网络通信的枢纽，既决定着网络的性能和效率，也决定着网络的安全和稳定。随着交换机技术的不断发展，交换机变得越来越成熟、越来越聪明、越来越强壮、越来越安全。

2.6.1　基于端口的传输控制

为了有效地保障网络传输安全，交换机内置了许多基于端口的传输控制，内容如下。

■　**广播风暴控制**

当端口接收到大量的广播、单播或多播包时，就会发生广播风暴。转发这些包将导致网络速度变慢或超时。借助于对端口的广播风暴控制，可以有效地避免硬件损坏或链路故障而导致的网络瘫痪。默认状态下，广播、多播和单播风暴控制被禁用。

■　**保护端口**

保护端口可以确保同一交换机上的端口之间不进行通信。保护端口不向其他保护端口转发任何数据包，包括单播、多播和广播包。传输不能在第二层保护端口间进行，所有保护端口间的传输都必须通过第三层设备转发。保护端口与非保护端口间的传输则不受影响。借助PVLAN 可以设置保护端口。

■　**端口安全**

端口安全，可以使用端口安全特性来限制进入一个端口的访问，从而避免非授权用户接入网络。可以为端口指定安全的 MAC 地址，或者指定所允许的最大安全 MAC 地址数。当将MAC 地址绑定至某个端口后，这个端口将不会转发源自其他 MAC 地址的包。如果限制安全

MAC 地址的数目为 1，并且绑定了唯一的源地址，那么连接在这个端口的主机将独自占有这个端口的全部带宽，如图 2-24 所示。

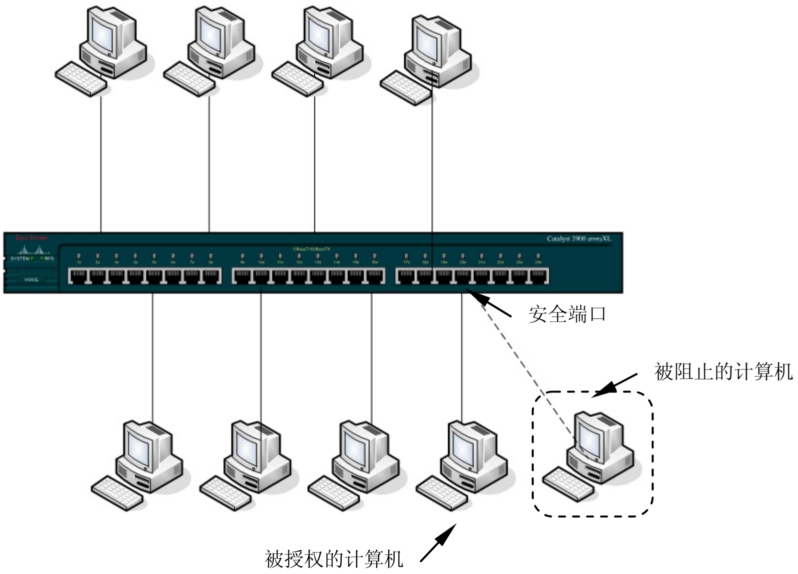


图 2-24　端口安全

2.6.2 Cisco IOS 防火墙

Cisco IOS 是思科网络设备的操作系统平台，被广泛应用于交换机、路由器、防火墙和无线设备。Cisco IOS 防火墙特性集通过在网络基础机构本身内提供安全访问策略，完善了 Cisco 的端到端安全产品，从而实现了独立设备不能提供的灵活性和控制水准。

■ **基本的和高级的通信过滤**

基本的和高级的通信过滤包括：

- 标准和扩展的访问控制列表（Access Control List，ACL）——将访问控制用于特定的网段，并定义哪些通信可以通过一个网段。
- 锁定和密钥动态的 ACL——根据用户身份（用户名/口令）授予通过防火墙的暂时访问。
- 基于策略的多端口支持——根据由安全策略决定的 IP 地址和端口，提供控制用户访问的能力。
- 网络地址转换（Network Address Translation，NAT）——通过对外界隐藏内部地址增强网络保密性；通过启动注册 IP 地址的保护，降低 Internet 访问的成本。
- 同级路由器验证——确保路由器从可靠的来源收到路由信息。
- 事件日志记录——通过将系统错误消息输出到一个控制台终端或系统日志服务器、设置严重级并记录其他参数，允许管理员实时跟踪潜在的违法或其他非标准活动。
- 虚拟专用网络（Virtual Private Network，VPN）——利用下列任何协议，通过公共线路（例如 Internet）提供安全的数据传输；降低远程分支办事处和外部网的实现及管

理成本；增强服务质量和可靠性；提供基于标准的互操作性。

- Cisco 加密技术——网络层加密功能，在传输期间防止通过网络窃取或窜改数据。
- IPSec——基于标准的网络层加密，提供数据保密性和验证。

■ **基于上下文的访问控制**

基于上下文的访问控制（Context-Based Access Control，CBAC）使管理员能够将防火墙智能实现为一个集成化单框解决方案的一部分。CBAC 通过严格审查源和目的地址，增强了使用众所周知端口（例如 FTP 和电子邮件通信）的 TCP 和 UDP 应用程序的安全。

CBAC 通过检查整个（数据）包了解应用程序状态信息，给 ACL 功能增加了智能检查。CBAC 利用这种信息创建一个暂时的、对话期特定的 ACL 入口，从而允许回返通信进入可靠网络。这种暂时的 ACL 有效地在防火墙中打开了一个大门。当一个对话期结束时，ACL 入口被删除，大门关闭。标准和扩展的 ACL 不能创建暂时的 ACL 入口，因此，难以确保为回返通信流量选择通道的先进应用程序的安全。

CBAC 比目前的 ACL 解决方案更加安全，因为它根据应用类型决定是否允许一个对话通过防火墙，并决定为回返通信流量是否从多个通道进行选择。之前，管理员仅通过编写 ACL 基本上使防火墙大门永久敞开，而借助 CBAC，可以在需要时打开防火墙大门，并在其他时候关闭大门，从而能够安全地许可多媒体和其他应用通信。

■ **Java 阻断**

随着大量 Java 小程序可用于 Internet，保护网络免受恶意小程序的攻击已经成为网络管理人员的一个主要课题。可以配置 Java 阻断来过滤或完全拒绝对没有嵌入在一个文档或压缩文件中的 Java 小程序的访问。

■ **服务拒绝检测和预防**

新近增强的服务拒绝检测和预防可以针对 SYN 泛滥、端口扫瞄和包注入提供网络防御。服务拒绝检测和预防可以检查 TCP 连接中的包顺序号。如果这些号码不在预期的范围内，路由器将撤消可疑的包。当路由器检测出新建包，它就发出一条警告信息。它还可以撤销半开的 TCP 连接状态表，以防止系统资源耗尽。

■ **审计跟踪**

增强的审计跟踪利用系统日志来跟踪所有事务；记录时间印迹、来源主机、目的地主机、所用的端口、对话，以及传输的总字节数。

■ **实时告警**

一旦查出可疑的活动，实时告警将向中央管理控制台发送系统日志错误信息。网络管理人员有能力立即对入侵作出反应。

2.6.3 IEEE 802.1x 认证

在传统的局域网环境中，只要有物理的连接端口，未经授权的网络设备就可以接入局域网，或者通过连接到局域网的设备进入网络，从而给企业造成了潜在的安全威胁。另外，在学校、智能小区等需要计费的网络中，验证用户接入的合法性也非常重要。IEEE 802.1x 作为解

决这个问题的良药，已经被集成到二层智能交换机中，可用于完成对用户的接入安全审核。

IEEE 802.1x 执行基于端口的网络访问控制。基于端口的网络访问控制使用交换的局域网（LAN）基础设施的物理特征来验证连接到 LAN 端口的设备，并防止访问身份验证进程已经失败的那个端口连接。IEEE 802.1x 身份验证用于对有线以太网和无线 IEEE 802.11 网络进行经过身份验证的网络访问。IEEE 802.1x 通过提供对集中式用户标识、身份验证、动态密钥管理和计账的支持来提高安全性和部署。

1. IEEE 802.1x 认证元素

在 IEEE 802.1x 协议中，只有具备了以下三个元素（如图 2-25 所示）才能够完成基于端口的访问控制的用户认证和授权。

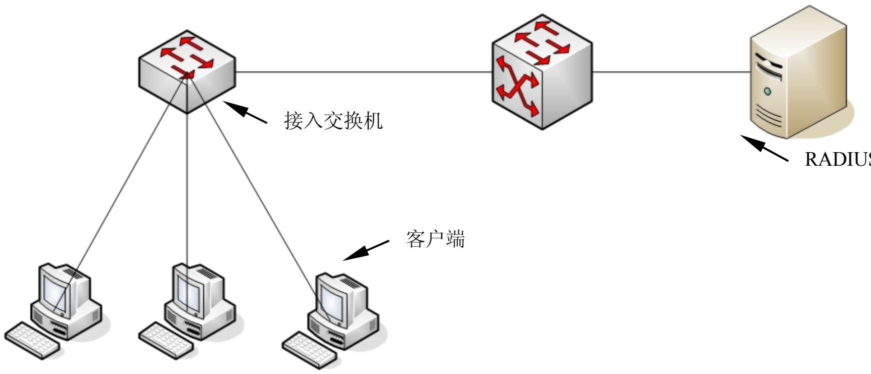


图 2-25 IEEE 802.1x 认证设备角色

- 客户端。一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。
- 认证系统。在以太网系统中主要是认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。
- 认证服务器。通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

802.1x 协议与 LAN 是无缝融合的。802.1x 利用了交换 LAN 架构的物理特性，实现了 LAN 端口上的设备认证。在认证过程中，LAN 端口要么充当认证者，要么扮演请求者。在作为认证者时，LAN 端口在需要用户通过该端口接入相应的服务之前，首先进行认证，若认证失败则不允许接入；在作为请求者时，LAN 端口则负责向认证服务器提交接入服务申请。基于端口的 MAC 锁定只允许信任的 MAC 地址向网络中发送数据。来自任何“不信任”设备的数据流会被自动丢弃，从而确保最大限度的安全。

2. IEEE 802.1x 认证过程

配置 IEEE 802.1x 基于端口的认证，必须启用认证、授权、计账（Authentication Authorization Accounting，AAA），以及认证方法列表。认证方法列表描述了查询和认证用户的次序与认证方法。

以下是 802.1x AAA 处理过程。

- 用户连接到交换机端口。
- 执行认证。
- 基于 RADIUS 服务器的 VLAN 分配被启用。
- 交换机将开始信息发送至计账服务器。
- 再次执行认证。
- 交换机发送临时计费更新信息到计账服务器。
- 用户从端口断开连接。
- 交换机发送终止信息到计账服务器。

第 3 章　交换机的选择与适用

就像梁桥、拱桥、斜拉桥、悬索桥等既功能相似，又各有其不同的特点和用途一样，交换机的种类非常之多，不仅彼此之间的性能差异较大，而且各自拥有不同的特点，分别适用于不同的场合。因此，必须根据实际环境和应用需要进行合理的选择。

3.1　交换机的分类与适用

根据不同的标准，可以对交换机作不同的分类。不同类型的交换机，各有其功能、特点和应用范围，因此，对于网络管理者而言，应当根据具体的使用环境和实际需求选择最恰当的交换机产品。

3.1.1　智能与傻瓜交换机

以交换机是否可管理为标准，可将其划分为智能交换机与傻瓜交换机。

1.　智能交换机

拥有独立的网络操作系统，可以进行配置和管理的交换机，称为智能交换机（也称可网管交换机）。

随着网络规模的扩大，接入计算机数量的增多，汇聚层交换机和核心层交换机必须选用可网管交换机，从而划分 VLAN、隔离广播域，提高数据传输效率，保障对敏感部门（总裁、财务、研发、人力资源等）的访问安全。对一些有较高性能和安全性需求，或者有较复杂网络应用的部门或工作组而言，也应当采用可网管交换机。

可网管交换机都有一个明显的特点，即都拥有一个“CONSOLE”端口，或者位于机箱的背板，或者位于机箱的前面板（如图 3-1 所示）。可网管交换机除了可以直接连接到交换机的 Console 口配置和管理外，还可以借助网络实现远程管理和维护。

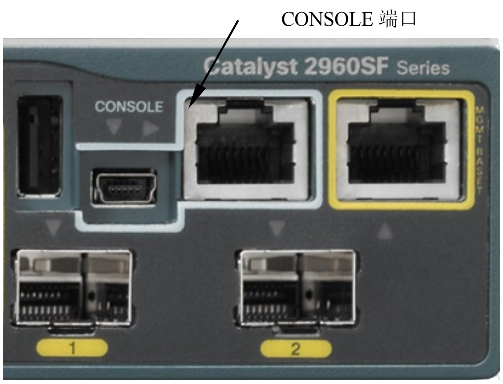


图 3-1　智能交换机

2.　傻瓜交换机

不能进行配置和管理的交换机，称为傻瓜交换机（也称不可网管交换机）。如果局域网络

对性能和安全性要求不是很高，那么工作组交换机可以选用不可网管交换机。由于傻瓜交换机价格非常便宜，因此被广泛应用于低端网络（如学生机房、网吧等）的接入层，用于提供大量廉价的网络接口。傻瓜交换机没有“CONSOLE”端口。图 3-2 所示为 D-Link 傻瓜交换机。

图 3-2　D-Link 傻瓜交换机

3.1.2 固定端口与模块化交换机

以交换机的结构为标准，可将其划分为固定端口交换机和模块化交换机。

1. 固定端口交换机

固定端口交换机虽然相对来说价格便宜一些，但是只能提供有限数量的固定端口（如 100Base-TX、1000Base-T、1000Base-SX 等）和固定类型的接口（如 StackWise 和 FlexStack 堆叠接口）或插槽（如 GBIC、SFP、X2、XFP 等插槽）。因此，无论从可连接的用户数量上，还是从可使用的传输介质上，都具有一定的局限性，通常作为接入层交换机，为普通用户提供网络接入；或者作为汇聚层交换机，实现接入层交换机之间的连接。图 3-3 所示为 Cisco Catalyst 3560 系列固定端口交换机，被用于为中高端用户提供网络接入。

图 3-3　Cisco Catalyst 3560 系列交换机

> **提·示**　如果交换机拥有 GBIC、SFP 或 XFP 等类型的插槽，可以根据需要选用不同标准的模块（如 1000Base-SX、1000Base-LX 或 1000Base-T 等），以适应多种类型的传输介质（双绞线、多模光纤、单模光纤等），从而拥有一定的灵活性。

2. 模块化交换机

模块化交换机（也称机箱交换机）虽然在价格上要昂贵得多，但拥有更大的灵活性和可扩充性，用户可任意选择不同数量、不同速率和不同接口类型的模块，以适应千变万化的网络需求。而且，模块化交换机都拥有很高的处理性能（背板带宽、转发速率和传输速率等）、很强的容错能力，支持交换模块的冗余备份，并且往往拥有可热插拔的双电源，以保证交换机的电力供应。因此，模块化交换机通常被应用于核心层交换机或汇聚层交换机，以适应大量的数据转发处理，以及复杂的网络环境和网络需求。图 3-4 所示为 Cisco Catalyst 4503 模块化交换机。

图 3-4　Cisco Catalyst 4503 模块化交换机

图 3-5 所示为应用于模块化交换机的 RJ-45 接口线卡（Line Card）。

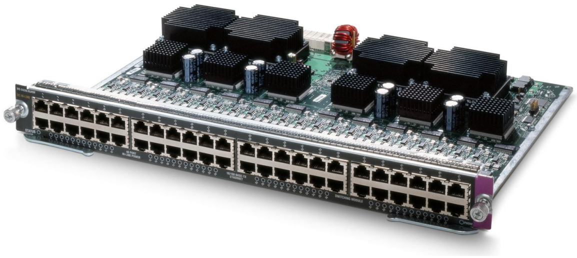


图 3-5　双绞线接口线卡

图 3-6 所示为应用于模块化交换机的 SFP 插槽线卡。

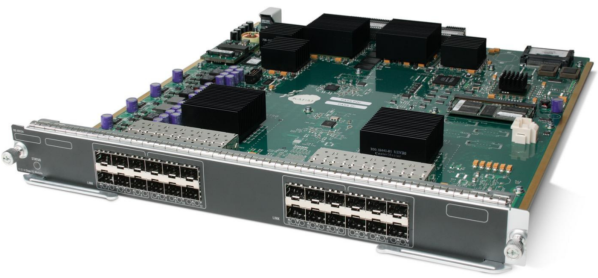


图 3-6　SFP 线卡

提·示 在选择交换机时，应按照网络需求和投入资金，综合考虑选择模块化交换机或固定端口交换机。一般来说，核心层交换机应考虑其扩充性、兼容性和排错性，因此，应当选用模块化交换机；而汇聚层交换机和接入层交换机则由于任务较为单一，故可采用简单的固定端口交换机。

3.1.3 接入层、汇聚层与核心层交换机

以交换机的应用规模或所处网络位置为标准，可以将网络交换机划分为接入层交换机、汇聚层交换机和核心层交换机，如图3-7所示。通常情况下，支持500个信息点以上大型网络应用的交换机为核心层交换机，支持300个信息点以下中型网络的交换机为汇聚层交换机，而支持100个信息点以内的交换机为接入层交换机。

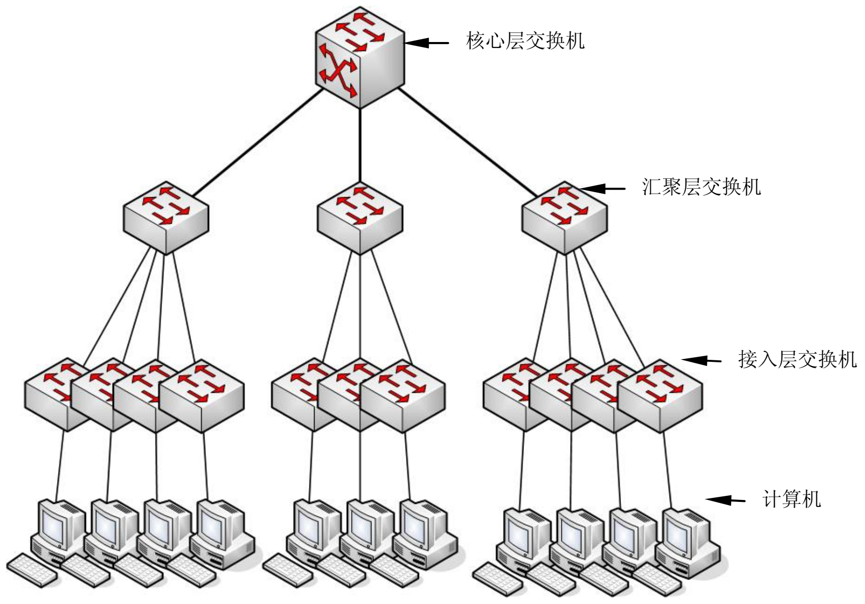


图3-7　不同位置的交换机

1. 接入层交换机

接入层交换机（也称工作组交换机）通常为固定配置端口交换机，拥有16～48个100Base-TX或1000Base-T以太网端口，用于实现普通计算机的网络接入。同时，还往往拥有2～4个1000 Mbps（甚至是10 Gbps）端口或插槽，用于实现与汇聚层交换机的千兆位（或万兆位）连接。图3-8所示为Cisco Catalyst 2960S系列接入层交换机。小型网络中的接入层交换机往往是

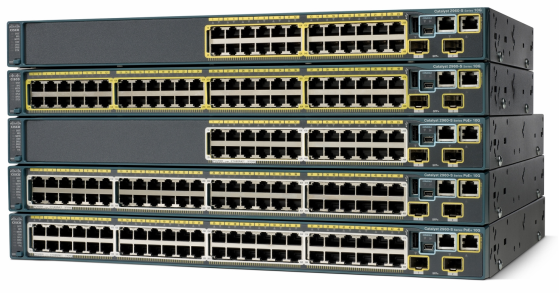


图3-8　Cisco Catalyst 2960S系列接入层交换机

不可管理的傻瓜交换机，而大中型网络中的接入层交换机则一般采用可网管交换机，以提高网络的安全性、稳定性和可管理性。

2. 汇聚层交换机

汇聚层交换机（也称部门交换机、骨干交换机或聚合交换机）是面向楼宇或部门接入的交换机，用于将接入层交换机连接在一起，并实现与核心层交换机的连接。汇聚层可以是固定配置，也可以是模块配置，一般有光纤接口。与接入层交换机相比，汇聚层交换机通常采用1000 Mbps 端口或插槽，并拥有 2～4 个 10 Gbps 端口或插槽。同时，具有网络管理的功能，可以通过计算机的串口直接连接，或者通过网络远程连接，实现对交换机的配置、监控和测试。支持基于端口的 VLAN，可实现端口管理，对流量进行控制。图 3-9 所示为拥有 8 个10 Gbps 热插拔上行链路模块的 Cisco Catalyst 4500-X 系列汇聚层交换机。

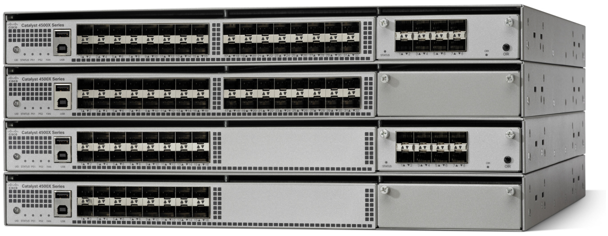


图 3-9　Cisco Catalyst 4500-X 系列汇聚层交换机

3. 核心层交换机

核心层交换机（也称企业交换机或中心交换机）属于高端交换机，全部采用模块化结构，可作为网络核心构建高速局域网。核心层交换机可以提供用户订制、优先级队列服务和网络安全控制，并能很快适应数据增长和改变的需要，从而满足用户的需求。对于有更多性能和安全需求的网络，核心层交换机不仅能传输海量数据和控制信息，更具有硬件冗余和软件可伸缩性特点，保证网络的可靠运行。图 3-10 所示为 Cisco Catalyst 6500E 系列核心层交换机。

图 3-10　Cisco Catalyst 6500E 系列核心层交换机

4. 数据中心交换机

数据中心交换机属于中高端交换机，中端采用固定配置（如 Cisco Nexus 2000、Nexus 3000、

Nexus 5000、Nexus 6000），高端采用模块化结构（如 Cisco Nexus 7000、Nexus 9000），主要用于连接网络服务器和网络存储设备。数据中心交换机提供 24～48 个 10 Gbps 和/或 40 Gbps 速率端口，40 Gbps 上联端口，支持二层和三层线速交换，适用于高性能数据转发。图 3-11 所示为 Cisco Nexus 2000 系列固定配置数据中心交换机，图 3-12 所示为 Cisco Nexus 7000 系列模块化数据中心交换机。

图 3-11　Cisco Nexus 2000 系列数据中心交换机

图 3-12　Cisco Nexus 7000 系列数据中心交换机

3.1.4 二、三、四层交换机

根据工作的协议层，交换机可分第二层交换机、第三层交换机和第四层交换机。

1. 第二层交换机

第二层交换机依赖于数据链路层中的信息（如 MAC 地址）完成不同端口数据间的线速交换，所有交换机都能够工作在第二层。接入层交换机通常全部采用第二层交换机。

2. 第三层交换机

第三层交换机具有路由功能，可以使用 IP 地址信息进行网络路径选择，并实现不同网段间数据的线速交换。当网络规模足够大，以至于不得不划分 VLAN 以减小广播所造成的影响时，只有借助第三层交换机才能实现 VLAN 间的线速路由。因此，在中小型网络中，核心层交换机通常都由第三层交换机充当，而大中型网络中的汇聚层交换机都选用第三层交换机。中高端固定端口的交换机，往往具有三层交换的功能，如 Cisco Catalyst 3850 系列、Catalyst 3750 系列、Catalyst 3650 系列（如图 3-13 所示）、Catalyst 3560 系列等。

图 3-13 Cisco Catalyst 3650 系列交换机

3. 第四层交换机

第四层交换机则使用传输层包含在每一个 IP 包包头的服务进程/协议（例如 HTTP 是用于传输 Web，FTP 是用于文件传输、Telnet 用于终端通信、SSL 用于安全通信等）进行交换和传输处理，实现带宽分配、故障诊断和对 TCP/IP 应用程序数据流进行访问控制等。由此可见，第四层交换机应当是核心层交换机的当然之选。Cisco Catalyst 4500 系列、Catalyst 4900 系列、Catalyst 6500 系列和 Catalyst 6800 系列（如图 3-14 所示）交换机都支持第四层交换技术。

图 3-14 Cisco Catalyst 6800 系列交换机

提·示 第二层交换机主要用于实现局域网内主机间的快速信息交流，第三层交换机主要用于实现 VLAN 间的线速转发，第四层交换技术则可以为网络应用资源提供最优分配，实现应用服务质量、负载均衡及安全控制。二、三、四层交换机并不存在谁要取代谁的问题，而是各有其针对的环境和应用的范围。

3.2 交换机的主要参数

局域网交换机是组成网络系统的核心设备。对用户而言，局域网交换机最主要的指标是端口的配置、数据交换能力、包交换速度等。下面将对交换机的一些重要技术参数作一些简要介绍，以便在设计网络拓扑结构和购置交换机时，根据网络的实际需要作出正确的选择。

3.2.1 三层交换机的主要参数

三层交换机主要被用于核心层交换机，以及大中型网络中的汇聚层交换机，承担着网络传输中的大部分数据流量的转发任务，决定着整个网络的传输效率。因此，三层交换机应当拥有较高的处理性能和可扩展性。Cisco 的 Catalyst 3850、Catalyst 3750、Catalyst 3650、Catalyst 3560 和 Catalyst 3550 系列都是三层交换机，Catalyst 6500、Catalyst 4900 和 Catalyst 4500 等四层交换机也都支持三层交换。

1. 转发速率

网络中的数据是由一个个数据包组成的，对每个数据包的处理要耗费资源。转发速率（也称吞吐量）是指在不丢包的情况下，单位时间内通过的数据包数量。吞吐量就像是立交桥的车流量，是三层交换机最重要的一个参数，标志着交换机的具体性能。如果吞吐量太小，就会成为网络瓶颈，给整个网络的传输效率带来负面影响。交换机应当能够实现线速交换，即交换速度达到传输线上的数据传输速度，从而最大限度地消除交换瓶颈。对于万兆位交换机而言，若欲实现网络的无阻塞传输，要求：

吞吐量（Mpps）=万兆位端口数量×14.88 Mpps＋千兆位端口数量×1.488 Mpps＋百兆位端口数量×0.1488 Mpps

如果交换机标称的吞吐量大于或等于上述计算值，那么在三层交换时应当可以达到线速。其中，1 个万兆位端口在包长为 64 B 时的理论吞吐量为 14.88 Mpps，1 个千兆位端口在包长为 64 B 时的理论吞吐量为 1.488 Mpps，1 个百兆位端口在包长为 64 B 时的理论吞吐量为 0.1488 Mpps。那么，这些数值是如何得到的呢？

事实上，包转发线速的衡量标准是以单位时间内发送 64 B 的数据包（最小包）的个数作为计算基准的。以千兆位以太网端口为例，其计算方法如下：

1 000 000 000 bps/ 8bit /（64＋8＋12）Byte = 1 488 095 pps

当以太网帧为 64 B 时，需考虑 8 B 的帧头和 12 B 的帧间隙的固定开销。由此可见，线速的千兆位以太网端口的包转发率为 1.488 Mpps。万兆位以太网的线速端口包转发率，正好为千兆位以太网的 10 倍，即 14.88 Mpps；而快速以太网的线速端口包转发率，则为千兆位以太网的十分之一，即 0.1488 Mpps。

例如，对于一台拥有 24 个千兆位端口的交换机而言，其满配置吞吐量应达到 24×1.488 Mpps = 35.712 Mpps，才能够确保在所有端口均线速工作时，实现无阻塞的包交换。同样，如果一台交换机最多能够提供 176 个千兆位端口，那么其吞吐量应当至少为 261.8 Mpps（176×1.488 Mpps=261.8 Mpps），这样才是真正的无阻塞结构设计。

图 3-15 所示为充当中小型网络核心层的 Cisco Catalyst 4500E 系列交换机，依据所采用管理引擎的不同，其转发速率有着较大的区别。例如，Supervisor Engine 8-E 转发速率为 250 Mpps、Supervisor Engine 7L-E 转发速率为 225 Mpps，Supervisor Engine V-10GE 转发速率为 102 Mpps、Supervisor Engine IV 转发速率为和 72 Mpps。对于 Cisco Catalyst 4507R+E 而言，尽管最多可以支持 240 个 1000 Mbps 端口或 68 个 10 Gbps 端口，但若欲实现线速转发，当采用 Supervisor

Engine 8-E 管理引擎时，其端口组合应当为 8 个 10 Gbps 端口＋88 个 1000 Mbps 端口；或者 168 个 1000 Mbps 端口。

图 3-15　Cisco Catalyst 4500-E 系列交换机

用于充当大中型网络核心层的 Cisco Catalyst 6500-E 系列交换机，依据所采用的管理引擎不同，其最大转发速率分别为 15 Mpps、210 Mpps 和 400 Mpps。以 Cisco Catalyst 6509 为例，尽管最多可以支持 32 个 10 Gbps 端口或 386 个 1000 Mbps 端口，但是，即使采用性能最好的管理引擎 Supervisor Engine 720，400 Mbps 的转发速率也只能支持 26 个 10 Gbps 端口，或者 268 个 1000 Mbps 端口的线速转发。

2.　背板带宽

带宽是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量，就像是立交桥所拥有的车道的总和。由于所有端口间的通信都需要通过背板完成，所以背板所能提供的带宽，就成为端口间并发通信时的瓶颈。带宽越大，提供给各端口的可用带宽越大，数据交换速度越快；带宽越小，给各端口提供的可用带宽越小，数据交换速度也就越慢。也就是说，背板带宽决定着交换机的数据处理能力，背板带宽越大，所能处理数据的能力就越强。因此背板带宽越大越好，特别是对那些汇聚层交换机和中心交换机而言。若欲实现网络的双全工无阻塞传输，必须满足最小背板带宽的要求。其计算公式如下：

背板带宽=端口数量×端口速率×2

Cisco Catalyst 4500-E 系列交换机依据插槽数量的不同，其背板带宽分别为 96 Gbps、240 Gbps 和 384 Gbps。根据上述公式计算，Catslyt 4510R-E 的 384 Gbps 的背板只能满足 192 个 1000 Mbps 端口的无阻塞并发传输，而 Catslyt 4503-E 的 96 Gbps 背板带宽，也就只能满足 48 个 1000 Mbps 端口的无阻塞并发传输。

提·示　对于三层交换机而言，只有转发速率和背板带宽都达到最低要求，才是合格的交换机，二者缺一不可。

3.　可扩展性

由于三层交换机往往充当核心层或汇聚层交换机，需要适应各种复杂的网络环境，因此

其可扩展性就显得尤其重要。可扩展性应当包括两个方面。

- 插槽数量。插槽用于安装各种功能模块和接口模块。由于每个接口模块所提供的端口数量是一定的，因此插槽数量也就从根本上决定着交换机所能容纳的端口数量。另外，所有功能模块（如管理引擎模块、IP 语音模块、扩展服务模块、网络监控模块、安全服务模块等）都需要占用一个插槽，因此插槽数量也就从根本上决定着交换机的可扩展性。
- 模块类型。毫无疑问，支持的模块类型（如 LAN 接口模块、WAN 接口模块、ATM 接口模块、扩展功能模块等）越多，交换机的可扩展性越强。仅以局域网接口模块为例，就应当包括 RJ-45 线卡、GBIC（Giga Bitrate Interface Converter）插槽线卡、SFP（Small Form Pluggable）插槽线卡、X2 插槽线卡等，以适应大中型网络中复杂环境和网络应用的需求。

如图 3-16 所示，Cisco Catalyst 6509-E 交换机拥有 9 个插槽，并且支持的模块类型有几十款，具有非常大的可扩展性，可适用于各种复杂的网络环境，并可满足各种网络应用需求，因此非常适宜充当大中型网络中的核心层交换机。

图 3-16　Cisco Catalyst 6509-E 交换机

如图 3-17 所示，Cisco Catalyst 3850 系列交换机可以根据需要安装 4 x Gigabit、4 x Gigabit Ethernet/2 x 10 Gigabit 或 4 x Gigabit Ethernet/4 x 10 Gigabit 的网络模块。Cisco Catalyst 3750-X 系列、Catalyst 3560-X 系列交换机也提供了 4 x Gigabit、2x 10 Gigabit SFP+插槽、2x 10GB-T、2x 10 Gigabit SFP+插槽和服务模块等网络模块。

图 3-17　Cisco Catalyst 3850 交换机

4. 系统冗余

第三层交换机作为网络核心或骨干，其工作状态的稳定性直接决定着网络的稳定性，而部件的物理损坏又是无法绝对避免的，因此交换机系统的部件冗余就显得尤其重要。通常情况下，电源模块、管理引擎等重要部件都必须提供冗余支持，从而保证所提供应用和服务的连续性，减少关键业务数据和服务的中断。如图 3-18 所示的 Cisco Catalyst 4507R-E 交换机就提供了电源模块和管理引擎的冗余。

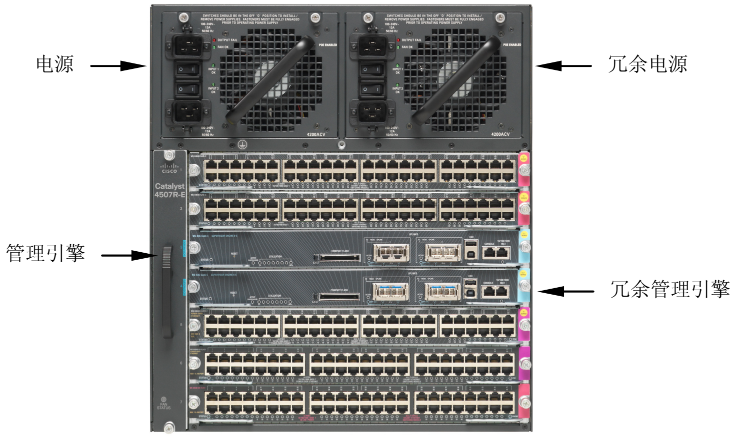


图 3-18 Cisco Catalyst 4507R-E 交换机

> **提·示** Catalyst 4507R/4510R 和 Catalyst 4507R-E/4510R-E 都支持管理引擎冗余。Catalyst 4507R/4510R 的管理引擎均安装在插槽 1 和插槽 2，Catalyst 4507R-E 的管理引擎安装在插槽 3 和插槽 4，Catalyst 4510R-E 则安装在插槽 5 和插槽 6。Catalyst 6500/6500E 系列交换机均支持管理引擎冗余，只是不同型号的机箱中管理引擎所使用的槽位有所不同。其中，3 和 4 插槽机箱使用插槽 1 和插槽 2，6 和 9 插槽机箱使用插槽 5 和插槽 6，13 插槽机箱使用插槽 7 和插槽 8。

图 3-19 所示的 Cisco Catalyst 3750-X 交换机也拥有冗余的电源和风扇，以最大限度地提高系统的稳定性。Cisco Catalyst 3850、Catalyst 3560-X 也拥有类似的冗余电源和风扇。

图 3-19 Cisco Catalyst 3750-X 交换机

5.　管理功能

交换机的管理功能（Management）是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。三层交换机必须支持 SNMP 协议，并且提供友好的设备管理界面。除了可以由厂商提供的网管软件管理外，还必须能够被第三方管理软件进行远程管理，实现与其他网络设备的统一管理，降低管理成本、简化管理操作。图 3-20 所示为 Catalyst 4506 交换机远程管理界面。

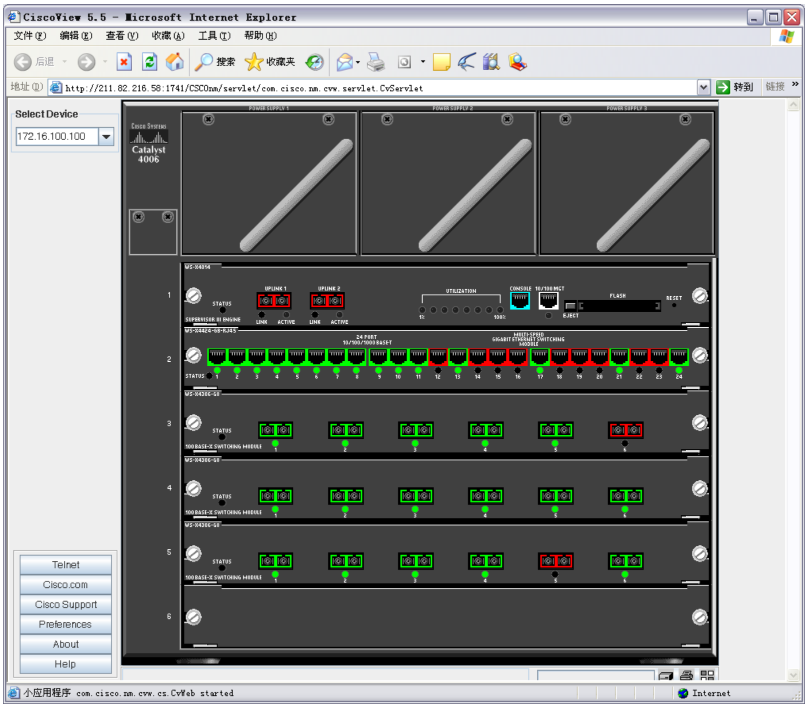


图 3-20　Cisco Catalyst 4506 交换机远程管理界面

3.2.2　二层交换机的主要参数

第二层交换机根据第二层数据链路层的 MAC 地址和 MAC 地址表来完成端到端的数据交换。第二层交换机只需识别数据帧中的 MAC 地址，直接根据 MAC 地址转发。第二层交换的解决方案，是一个“处处交换”的方案，虽然该方案也能划分子网、限制广播、建立 VLAN，但它的控制能力较小、灵活性不够，也无法控制流量，缺乏路由功能。因此只能被用于充当接入层交换机。Cisco 的 Catalyst 2960 系列、Catalyst 2950 系列，都是二层交换机。

1.　端口类型

交换机常见的端口有 3 种类型，即光纤端口、双绞线端口和插槽（如 GBIC 插槽、SFP 插槽、SFP+插槽和 XFP 插槽）。为了增加连接的灵活性，适应更加复杂的网络环境，光纤端口已经逐渐被 SFP、SFP+或 XFP 插槽所取代。由于二层交换机主要用于接入层，上连同一建筑内的汇聚层交换机，下连普通用户的计算机，传输距离都非常有限，因此通常只需拥有 RJ-45

接口（100Base-TX 或 1000Base-T）即可。当然，若欲实现与上层交换机（如核心层交换机或汇聚层交换机）的远程连接，或与其他交换机之间的千兆位或万兆位连接，也应当拥有 SFP、SFP+或 XFP 插槽。

> **提·示** 有关端口类型的详细内容，请参见本书“第 4 章 交换机的端口与连接”相关部分。

2. 端口速率

从端口速率看，主要有 100 Mbps 和 1000 Mbps 两种，个别接入交换机也提供 10 Gbps 端口。常见的搭配形式有 n×10/100 Mbps、n×1000 Mbps+m×100 Mbps、n×1000 Mbps、n×10 Gbps+ m×1000 Mbps 等四种。

n×100 Mbps 交换机所有端口全部为 100 Mbps 端口。桌面式交换机通常为 8 个端口，机架式交换机通常为 12、16、24 或 48 个端口。该类交换机是价格低廉的主流产品之一，大多为傻瓜交换机产品，被广泛地作为低端网络中的工作组交换机，为网络内的普通计算机提供接入服务。图 3-21 所示为拥有 12 个 100 Mbps 端口的 Cisco Catalyst 2950-12T 接入层交换机。

图 3-21 n×100 Mbps 交换机

n×1000 Mbps+m×100 Mbps 交换机拥有 2 或 4 个 1000 Mbps 端口或插槽，以及 24 或 48 个 100 Mbps 端口。由于可实现与其他交换机的千兆位连接，从而有效地解决了交换机之间的互连瓶颈。随着千兆位端口价格的不断下降，该类交换机的性价比越来越高，被广泛应用于对安全性和可管理性要求较高的接入层交换机。图 3-22 所示为 Cisco Catalyst 2960-Plus 系列接入层交换机，均拥有 2 个 1000 Mbps 端口和 SFP 插槽。

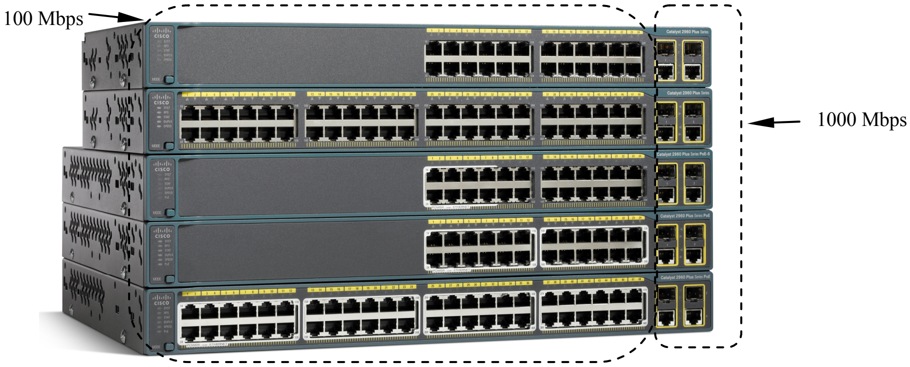


图 3-22 n×1000 Mbps+m×100 Mbps 交换机

提·示　图 3-20 中两款交换机貌似拥有 4 个 1000 Mbs 端口，不过，SFP 插槽与 RJ-45 端口为复用端口，即只能使用其中的任意一个，两者不能同时使用。所以，1000 Mbps 端口实际上仍然为 2 个。

n×1000 Mbps 交换机全部采用 1000 Mbps 端口或插槽，一般为 24 或 48 个 1000Base-T 端口，以及 2 或 4 个 1000 Mbps 插槽。毫无疑问，千兆位的带宽能够完美实现任何网络功能，完全满足各种形式的网络需求。同时，SFP 插槽又可以提供足够的网络连接的灵活性，因此，是搭建高性能网络的当然之选。图 3-23 所示为 Cisco Catalyst 2960-S 系列接入层交换机，所有端口全部为 1000 Mbps。

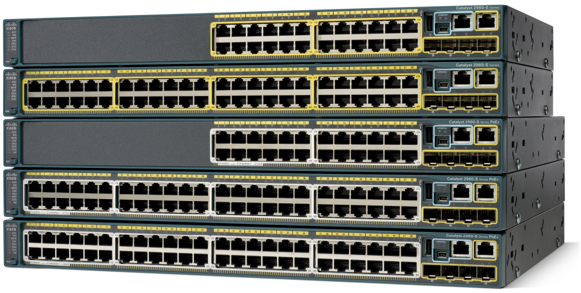


图 3-23　*n*×1000 Mbps 交换机

n×10 Gbps+ *m*×1000 Mbps 交换机拥有 2 或 4 个 10G bps 端口或插槽，以及 24 或 48 个 1000 Mbps 端口。向上实现与汇聚交换机的万兆连接，向下为计算机提供高速的千兆位连接，被广泛应用于对传输速率要求较高的接入层交换机。图 3-24 所示为 Cisco Catalyst 2960-X 系列接入层交换机，拥有 2 个 10 Gbps Uplink 端口。

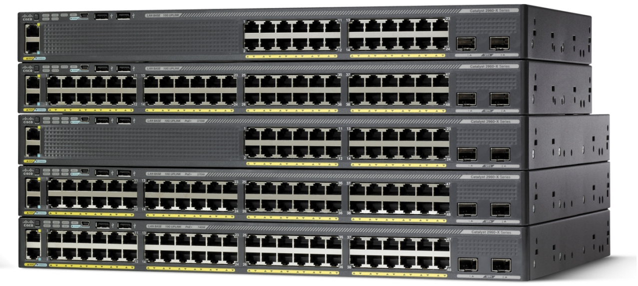


图 3-24　*n*×10 Gbps+ *m*×1000 Mbps 交换机

提·示　交换机的端口属性主要包括两个方面，一个是端口数量，一个是端口类型。在选择端口数量时，应当掌握以下两个基本原则：

- 适当冗余。端口数量越多，交换机的价格越高。所以，应当根据接入计算机的数量确定端口，并为未来接入的用户预留适当数量的端口。
- 高密度。由于交换机之间的互连会导致端口的浪费，因此应当尽量选择 24 或 48 端口交换机。

3. 延时

交换机延时（Latency）也称为延迟时间，是指从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔，所采用的转发技术等因素均会影响延时。延时越小，数据的传输速率越快，网络的效率也就越高。特别是对于多媒体网络而言，较长的数据延迟，往往导致多媒体的短暂中断，所以交换机的延迟时间越短越好。

4. MAC 地址数

不同交换机每个端口所能够支持的 MAC 数量不同。在交换机的每个端口，都有足够内存（Buffer）记忆多个 MAC 地址，从而“记住”该端口所连接站点的情况。由于 Buffer 容量的大小限制了这个交换机所能够提供的交换地址容量，所以当该端口所容纳的计算机数量超过了地址容量时，目的站的 MAC 地址将很可能并没有保存在该交换机端口的 MAC 地址表中，那么该帧即将以广播方式发向交换机的每个端口。当这种情况频频发生时，将在很大程度上影响网络中数据的传输效率。不过，对于接入层交换机而言，由于实施通信的计算机和网络设备的数量有限，所以只要能够记忆 1024 个 MAC 地址基本上就可以了，而一般的交换机通常都能做到这一点。

5. VLAN 表项

VLAN 的主要作用有两点，一是将大的网络划分为若干小的子网络，从而减少广播提高网络传输效率；二是提高网络安全性，控制用户对某个子网络的访问，有效地保护敏感数据。VLAN 表项限制了网络内可容纳的 VLAN 数量，以及对 VLAN 访问控制的能力。如果 VLAN 表项较小，将限制对 VLAN 的划分，从而不适宜于安全和应用较为复杂的网络。

6. 扩展方式

交换机扩展端口的方式有两种，一是级联，二是堆叠。采用级联方式时，交换机之间只能借助一个端口通信，从而使得交换机之间的连接成为网络瓶颈。采用堆叠方式时，借助于专用的模块和电缆，可以堆叠交换机间的高速无阻塞连接，并可实现统一配置与管理。显然，堆叠更适合为大量的计算机提供接入服务，通常被接入层交换机所采用。无论是二层的 Cisco Catalyst 2950/2960 系列，还是三层的 Cisco Catalyst 3550/3560 系列和 Catalyst 3850/3750 系列交换机，都是既支持级联又支持堆叠。图 3-25 所示为 Cisco Catalyst 2960-SF 系列交换机。

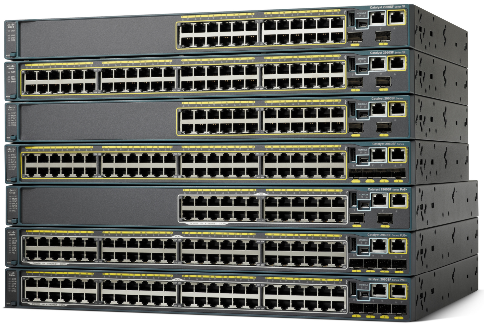


图 3-25　Cisco Catalyst 2960-SF 系列交换机

7. 链路汇聚

使用端口聚合协议，可以将多个端口绑定在一起，从而成倍地增加连接带宽，并实现链路备份，以及端口间的负载均衡，保证交换机在几秒钟内快速从失败中恢复。

链路汇聚技术是将多台设备之间的多条物理链路捆绑为一个逻辑链路，使得该逻辑链路的容量为所有物理链路的容量之和。同时，当其中一条物理链路中断时，整个逻辑链路也不会中断，大大地提高了网络连接的可靠性。因此，链路汇聚技术也经常被用于接入层交换机与汇聚层交换机之间，尤其是没有千兆位级联的端口的交换机，在提高向上级联带宽的同时，还可以提高网络的稳定性和可用性。图 3-26 所示为只拥有 1000 Mbps 端口的 Cisco Catalyst 接入交换机与汇聚交换机之间采用 4 条链路绑定，从而实现接入层交换机与汇聚层交换机之间 4000 Mbps 的连接带宽，保证了所连接计算机与网络骨干的高速连接。

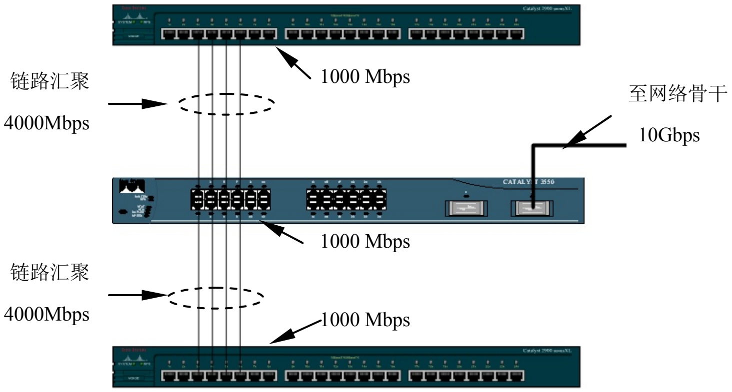


图 3-26 链路汇聚

8. 管理功能

应用于大中型网络中的交换机应当都拥有管理功能，并且能够被第三方管理软件所管理。可网管交换机借助 VLAN、扩展树、QoS、端口聚合等，用于实现广播域的划分、冗余链路的智能选择、服务质量控制，以及将若干端口绑定在一起以成倍地增加网络带宽，从而适应大中型网络对网络安全、网络应用、网络控制和网络管理的需要。

3.3 交换机的选择策略

针对不同的网络需求和投资额度，可以选择不同型号的网络设备，以满足用户对连接带宽、转发速度、稳定性和安全性等不同的需求。

3.3.1 可网管交换机的选择

可网管交换机通常拥有独立的操作系统，可以借助配置启用一些高级的网络功能，从而实现网络的稳定运行、访问安全，以及复杂的网络应用。通常情况下，可为其指定管理 IP 地址信息，从而实现远程管理，甚至使用网管软件进行统一配置、监视和管理的交换机。Cisco

Catalyst 系列交换机全部为可网管交换机（如图 3-27 所示）。

图 3-27　Cisco Catalyst 系列交换机

1. 可网管交换机的特点

可网管交换机具有以下特点。

- 提高网络稳定性。傻瓜式交换机不能构建冗余网络，否则将由于存在拓扑环而导致网络瘫痪。由于没有线路冗余，所以当线路、设备或模块损坏后，就有可能导致某一部分网络、甚至是整个网络的通信中断。可网管交换机借助 Spanning Tree（扩展树）和 EtherChannel 等技术，不仅可以实现链路的冗余，甚至可以成倍地增加设备之间（交换机之间、交换机与路由器之间、交换机与服务器之间）的连接带宽，并实现网络负载均衡，从而确保了网络运行的稳定。
- 提高网络安全性。傻瓜交换机没有任何安全性可言，而可网管交换机可使用 VLAN（虚拟网）、PVLAN（专有虚拟网）和 ACL（访问列表）等多种方式，将不同部门的网络隔离开来，拒绝某些用户对敏感数据的访问，从而保障数据的存储和访问安全。另外，借助于访问列表，还可以有效地拒绝蠕虫病毒的传播，限制某些用户的访问权限，从而进一步保证了网络安全。
- 提高网络传输效率。当网络内的计算机数量足够多，并且使用的网络协议也足够多时，会产生大量的广播包，从而严重影响网络的传输效率。借助于可网管交换机的 VLAN 功能，可以将一个网络划分为若干逻辑子网，缩小广播域的范围，从而提高整个网络的传输效率。而傻瓜交换机只能划分碰撞域，却无法划分广播域，从而不能用于单独构建计算机数量多于 150 台的网络。
- 支持复杂网络应用。可网管交换机全面支持 QoS（服务质量），可以根据数据传输的不同类型，由管理员指定数据传输的优先级别，从而确保了视频会议、IP 电话等实时传输的网络应用的需要。在由傻瓜交换机构建的网络中，无论什么数据都要依次排除等待，从而无法适应多媒体等特殊的网络应用。如图 3-28 所示为支持无线网络和 VoIP 语音电话的 Cisco Catalyst 4500-E 交换机。

图 3-28　Cisco Catalyst 4500-E 交换机

- 支持远程监视与管理。一旦为可网管交换机配置了 IP 地址，就可以实现对该交换机的远程监视、配置和管理。对于大中型网络而言，这一点非常重要。这也就意味着，网管只需坐在自己的计算机前，就可以实现对网络中所有交换机的管理，了解交换机的运行状态，并根据需要修改交换机的配置。许多可网管交换机不仅可以借助网管软件（如 HP OpenView、CisocWorks）进行统一管理，甚至可以将由若干交换机构成的堆叠当做一台交换机管理，从而降低了管理的难度与强度。

2. 可网管交换机的应用

虽然可网管交换机与不可网管交换机在外观上基本没有差别，但由于性能和功能上的差别，可网管交换机的价格往往是傻瓜交换机价格的 5 倍甚至更高。所以，可网管交换机通常都被用于比较重要的位置。当然，如果资金比较充裕，也可以在整个网络中都使用可网管交换机，从而实现对网络中每一台计算机的访问控制。可网管交换机在网络中的应用如图 3-29 所示。

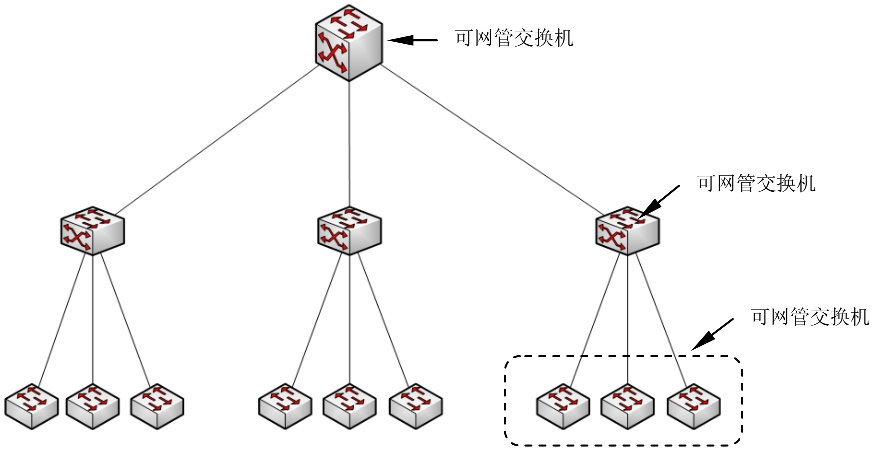


图 3-29　可网管交换机在网络中的应用

- 核心层交换机。作为网络核心和枢纽的核心层交换机必须选用可网管交换机，而且应当选用三层可网管交换机。原因很简单，所有的网络应用和网络安全都必然会经过核心交换机，因此核心交换机从根本上决定着网络性能，以及所能提供的网络应用。另外，每个大中型网络都需要配置 VLAN，而 VLAN 之间的通信必须借助三层设备才能实现，三层交换机则被用于实现 VLAN 之间的线速转发。
- 汇聚层交换机。汇聚层交换机大多被放置于每栋建筑物，用于连接接入层交换机。一栋建筑内往往拥有多个部门、需要实现各种不同的网络应用。因此，若欲实现与核心交换机的冗余连接，保障网络连接的稳定；实现 VLAN 划分，实现网络访问的安全；就必须采用可网管交换机。
- 重要的接入层交换机。接入层交换机用于直接连接计算机。如果交换机所连接的计算机都属于同一类型的用户，并且彼此之间没有对数据访问的限制，那么完全可以采用傻瓜交换机。相反，如果所连接的用户对网络安全有着较高的要求，或者网络应用比较复杂，必须实现对交换机每个端口的控制，那么就必须采用可网管交换机。

3. 选购时应当考虑的问题

不同位置、不同环境、不同应用需要不同的网管交换机。因此，在选购可网管交换机时，应当考虑以下问题。

- 所处位置。不同位置应当选用不同的可网管交换机。中心交换机应当选择模块化的四层或三层交换机，汇聚层交换机建议选择高性能的、固定配置的三层交换机，而工作组交换机则一般选择二层交换机，网络应用较为复杂、安全性要求严格、对传输性能要求较高的接入层交换机，也可选择中低端的三层交换机。
- 网络应用。不同的网络应用决定着所需设备的性能。性能越高的交换机自然价格也就越高，因此不要盲目追求高性能，而应当根据网络应用、数据流量等诸多因素，选择最适合网络应用的、最具性价比的交换机。当然，适当地性能冗余还是必须的。
- 所处环境。在选购交换机时，不能将它们相互割裂开来，而应当综合地、联系地进行考虑。考虑下级交换机是否支持上级交换机的功能与应用，考虑上下级交换机在性能上应有的差别，考虑上下级交换机端口的类型与数量，考虑传输距离、网络带宽和通信线缆，从而使所有交换机相互协调，达到彼此之间的最佳组合。
- 设备兼容性。尽管不同的可网管交换机大多遵守相同的国际标准，但每个厂家都有一些特殊的协议，并且使用不同的网络管理软件，因此，若欲实现对可网管交换机的统一管理，实现各种复杂的网络应用，达到性能最优化，就应当尽量选择同一厂商的产品。
- 设备性能。设备性能也是在选购交换机时必须注重的因素。其中，背板带宽、转发速率、VLAN 数量、MAC 地址数量、插槽数量、支持的端口类型、堆叠层数等参数，都必须根据交换机所处的位置与网络应用确定。

3.3.2 不同位置交换机的选择

1. 核心层交换机的选择

局域网络绝大部分的流量都是对网络服务器和 Internet 的访问，而服务器和 Internet 设备往往都直接连接在核心层交换机上，或者通过核心交换机再连接到汇聚交换机上。因此，作为网络核心的核心层交换机无时无刻不在承受着巨大的流量压力，其处理性能将决定着整个网络的传输效率。因此，对核心层交换机的选择也就显得尤其重要。Cisco 的 Catalyst 6800 系列、Catalyst 6500 系列、Catalyst 4900 系列和 Catalyst 4500 系列，均可以分别充当大中型网络中的核心层交换机。

选择核心层交换机时，应当注重考察以下几个参数。

■ **扩展能力**

核心层交换机应当全部采用模块化结构，必须拥有相当数量的插槽，具有强大的网络扩展能力，以保护原有的投资，在网络扩展或应用需求发生变化时，只需更换或添加线卡或模块即可满足新的需求。毫无疑问，模块化结构拥有更强劲的性能、更大的灵活性和可扩充性，可以根据现实的或未来的需要选择不同数量、不同速率和不同接口类型的模块，以适应千变万化

的网络需求。

■ **处理性能**

由于网络内 80%的数据流量都发生在核心层交换机上，因此，核心层交换机应当拥有强劲的处理能力，即拥有较高的背板带宽和转发速率，以保证数据的无阻塞转发和路由。否则，核心层交换机就会成为整个网络的瓶颈。如图 3-30 所示为 Cisco Catalyst 4500-E Supervisor Engine 8-E 管理引擎，提供高达 928 Gbps 的背板带宽，每插槽 48 Gbps 无阻塞传输，8 个无阻塞 10 Gbps 上行链路。同时，还内置有无线控制器，支持高达 20 Gbps 无线吞吐量，50 个无线访问点，2000 个无线客户端。

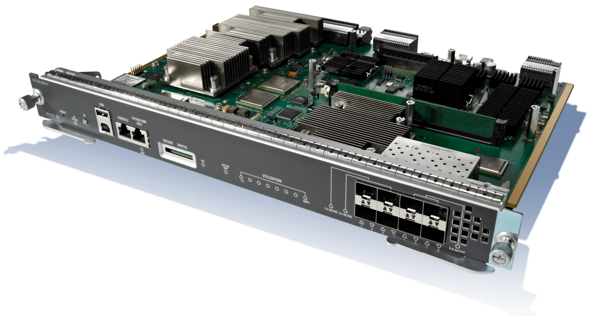


图 3-30 Cisco Catalyst 4500-E Supervisor Engine 8-E 管理引擎

■ **多层交换**

核心层交换机应当同时支持三层交换和四层交换。

三层交换用于实现局域网络中 VLAN 之间的线速转发。虚拟网的主要作用有两点，一是将大的网络划分为若干小的子网络，从而减少广播提高网络传输效率；二是提高网络安全性，控制用户对某个子网络的访问，有效地保护敏感数据。由于虚拟 VLAN 之间无法直接通信，因此必须借助于拥有路由功能的三层交换机，以硬件方式可以实现虚拟网之间的线速转发，解决虚拟网之间的传输瓶颈，从而可以有效地解决网络安全和传输效率的问题，使虚拟网络的广泛应用成为可能。

四层交换用于实现对网络服务的快速访问。在四层交换中，决定传输的依据不仅仅是 MAC 地址（OSI 模型第二层）或源/目标 IP 地址（OSI 参考模型第三层），而且包括 TCP/UDP（OSI 参考模型第四层）应用端口号，被设计用于高速 Intranet 应用。四层交换除了负载均衡功能外，还支持基于应用类型和用户 ID 的传输流控制功能。

■ **冗余能力**

冗余能力是网络安全运行的保证。任何厂商都不能保证其产品在运行的过程中不发生故障。而故障发生时能否迅速切换就取决于设备的冗余能力。对于核心层交换机而言，重要部件都应当拥有冗余能力，比如管理引擎冗余、电源冗余、风扇冗余等（如图 3-31 所示）。另外，还必须支持链路冗余和路由冗余，这样才能在最大程度上保证网络稳定运行。

图 3-31　冗余模块

■　**安全性能**

核心层交换机应当支持 IEEE 802.1x 基于端口的访问控制，支持本地和远端认证，EAP 终结或者透传；支持 RADIUS 和 TACACS+认证，支持 MAC 访问列表、IP 访问列表和 VLAN 访问列表，并支持私有 VLAN。可实现基于时间段控制，并限制每端口最大用户数。图 3-32 所示为 Cisco Catalyst 交换机认证方式设置页面。

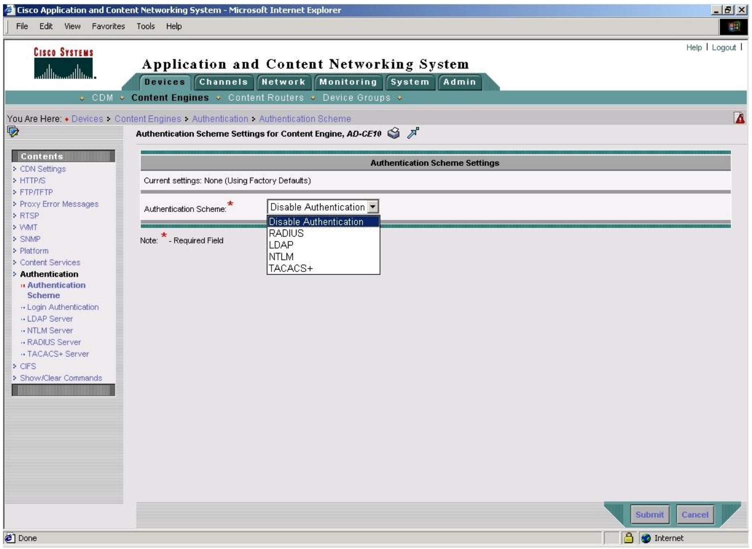


图 3-32　认证设置页面

2.　汇聚层交换机的选择

由于汇聚层交换机通常只用于连接同一座建筑内的工作组交换机，或者用于连接网络服务器，因此对端口数量通常没有太多的要求。但是，对端口速率、背板带宽、网络功能等要求较高，以获得高速、稳定的网络骨干。Cisco 的 Catalyst 4500 系列、Catalyst 4900 系列，均可以充当楼宇或部门的汇聚层交换机。网络规模不大的中小型网络，也可采用 Catslyst 3850 系列或 Catalyst 3750 系列作为汇聚层交换机。

选择汇聚层交换机时，应当注重考察以下几个参数。

■　**背板带宽**

背板带宽作为交换机的重要参数之一，决定着交换机是否能够实现二层交换的线速转发。例如，Cisco Catalyst 4900 系列有 3 款产品，分别为 Catalyst 4948、Catalyst 4948-10GE 和 Catalyst 4900M（如图 3-33 所示），分别最多拥有 48 个、48 个或 40 个 1000 Mbps 端口；或者最多拥有 0 个、2 个和 24 个 10 Gbps 端口，背板带宽分别为 96 Gbps、136 Gbps 和 320 Gbps，完全可以满足线速交换的需要。

图 3-33　Cisco Catalyst 4900M 交换机

■　**三层交换**

对于较大规模的网络，为了减轻核心层交换机的负担，汇聚层交换机通常采用三层交换机，从而实现楼宇内或部门内的数据交换。特别是对于那些划分为有若干 VALN，同时大量访问就发生在楼宇内或部门内的子网而言，汇聚层交换机选用拥有三层交换技术的设备就显得更有必要。需要注意的是，当汇聚层采用三层交换机时，汇聚层与核心层之间的端口将不能再配置为 VLAN Trunk 端口，而只能配置为路由端口，如图 3-34 所示。

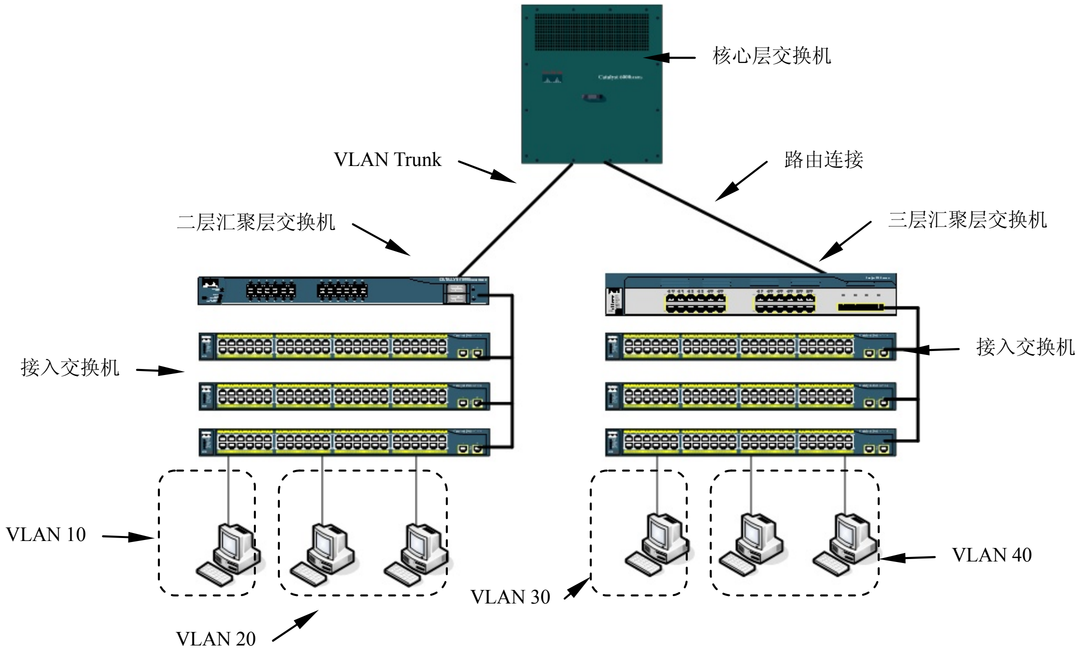


图 3-34　汇聚层采用三层交换机

■ **链路汇聚**

汇聚层交换机作为核心层交换机和接入层交换机的桥梁，起着承上启下的重要作用。如果接入层交换机不拥有千兆位以太网端口，那么为了避免向上级联时的网络瓶颈，采用链路汇聚成倍地增加网络带宽似乎是唯一正确的选择。同时，为了保证汇聚层交换机与核心层交换机连接的高速和稳定，采用链路汇聚技术，不仅可以增加网络带宽，而且还可以避免由于端口或链路故障而导致的通信失败。

■ **端口类型**

汇聚层交换机对网络端口具有以下要求。

- 因为是连接接入层交换机的交换机，所以汇聚层交换机必须拥有大量的千兆位以太网端口。
- 由于垂直布线往往采用光纤，因此汇聚层交换机应当有较多的 SFP、SFP+或 XFP 插槽。如果与接入层交换机距离非常近（例如，安装在一个机柜中），并且电磁干扰并不严重，也可以选择采用 RJ-45 端口。
- 由于汇聚层交换机又必须连接至核心层交换机，因此为了避免在上连链路中产生网络瓶颈，在投资额允许的情况内，可以选择 10 Gbps 端口的产品。

> **提·示** 如果汇聚层交换机同时用于直接连接少量计算机，并且网络内的流量也不太大，也可以是全 1000 Mbps 端口的形式。

3. 接入层交换机的选择

接入层交换机用于直接连接计算机或其他网络终端，因此对性能要求往往并不太高，只是需要较多数量的 RJ-45 端口。Cisco 的 Catalyst 2960 系列、Catalyst 2950 系列，以及 Catalyst 3750 系列、Catalyst 3650 系列、Catalyst 3560 系列和 Catalyst 3550 系列，均可作为接入层交换机。

选择接入层交换机时，应当注重考察以下几个参数。

■ **端口类型**

接入层交换机对网络端口具有以下要求。

- 接入层交换机通常只用来连接计算机或其他网络终端，而且就目前情况来看，100 Mbps 速率基本可以胜任所有的网络需求，同时水平布线和工作区布线全部采用双绞线，因此其主要端口应当是 100Base-TX 端口。当接入计算机的访问量较大时，也可以考虑采用 1000 Mbps 接口产品。
- 交换机端口数量越多，所连接的计算机数量越多，浪费的端口数量越少。所以，通常情况下，应当选择 24 口或 48 口，以减少交换机的使用量。
- 为了保证所连接的设备能够无阻塞地访问骨干网络，接入层交换机还应当拥有少量（2～4 个）SFP 插槽或 1000Base-T 等 1000 Mbps 端口，甚至 XFP 或 SFP+等 10 Gbps 插槽。端口类型视与汇聚层交换机的连接距离、垂直布线所采用的传输介质（光纤还是双绞线），以及电磁干扰的强度而定。

如图 3-35 所示的 Cisco Catalyst 2960 系列交换机，都拥有 2 个或 4 个千兆位以太网端口，

和 24 个或 48 个 100 Mbps 端口。因此，既可以连接大量的计算机终端，又可以实现与汇聚层交换机的高速连接。同时，还可以选择使用 SFP 插槽或 RJ-45 端口，以适应光纤链路和双绞线链路，从而拥有相当大的灵活性，因此应当作为接入层交换机的当然之选。

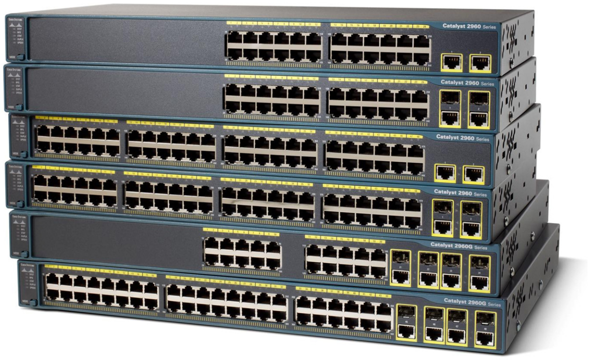


图 3-35 Cisco Catalyst 2960 系列交换机

■ **延扩方式**

当接入的计算机数量非常多（如学生机房、营业大厅等），垂直布线或汇聚层交换机的端口数量又有限时，往往只能采用堆叠或级联的方式实现接入层计算机之间的连接。如果大量访问都产生在子网内部，建议选择可以堆叠的交换机。否则，也可选择不可堆叠交换机，从而借助级联方式实现彼此之间的连接。Cisco Catalyst 2950、Catalyst 2960、Catalyst 3550、Catalyst 3560、Catalyst 3650 和 Catalyst 3750 系列，均可实现彼此之间的堆叠。

■ **网络管理**

如果网络对传输性能和网络安全要求较高，那么接入层交换机应当全部采用可网管交换机，从而实现对每个网络端口和每台交换机的管理。

提・示

可网管交换机的价格为傻瓜交换机的 2～5 倍。对于一些普通接入的计算机用户（如学生机房、网吧等场所），只需采用少量可网管交换机，然后将其他不可网管交换机分别级联在可网管交换机上，从而实现对网络用户的分组（连接至同一傻瓜交换机上的计算机为一组）管理，获得最佳性价比。

第 4 章　交换机的端口与连接

毫无疑问，交换机是借助各种端口实现与其他网络设备、终端设置连接的。那么，交换机究竟有哪些端口类型？各有什么特点？这些端口之间应当如何连接？又使用什么连接在一起呢？只有搞清楚这些问题，才能将搭建局域网的问题落到实处。

4.1　IEEE 802.3 系列标准

所有类型的以太网端口都是在 IEEE 802.3（Institute of Electrical & Electronic Engineers，电气和电子工程师协会）标准上发展和完善起来的。因此，若欲掌握以太网端口技术，就不能不了解 IEEE 802.3 系列标准。

4.1.1　10 Mbps 以太网标准

10 Mbps 以太网（Ethernet）执行 IEEE 802.3 标准，传输数据的方式为 CDMA/CD，可使用光纤、双绞线、细缆和粗缆作为传输介质。

传统的 10 Mbps 以太网拥有 4 种标准。

- 10Base-5：传输速率为 10 Mbps 的粗缆网络，区段最大长度为 500 m。
- 10Base-2：传输速率为 10 Mbps 的细缆（RG-58A/U）网络，区段最大长度为 185 m。
- 10Base-T：传输速率为 10 Mbps 的双绞线网络，从计算机到集线设备的最远传输距离为 100 m，使用三类以上屏蔽或非屏蔽双绞线。
- 10Base-F：传输速率为 10 Mbps 的光缆网络主干，光端口间的最远传输距离为 4 km。使用 1 对多模光纤传输。

由于所提供的传输速率太低，无法满足网络用户对多媒体等大流量数据传输的需要，所有基于 IEEE 802.3 标准的应用产品已经被淘汰。

4.1.2　100 Mbps 快速以太网标准

1995 年，IEEE 通过了 802.3u 标准，将以太网的带宽扩大为 100 Mbps，称之为快速以太网（Fast Ethernet）。

快速以太网主要有 2 种标准。

- 100Base-TX，传输速率为 100 Mbps 的双绞线网络，从计算机到集线设备的最大距离为 100 m。采用五类及以上屏蔽或非屏蔽双绞线，使用其中的 2 对（1/2 线和 3/6 线）进行传输。图 4-1 所示为超五类

图 4-1　超五类非屏蔽双绞线

非屏蔽双绞线。

- 100Base-FX，传输速率为 100 Mbps 的光缆网络主干。采用 1 对多模光纤传输时，最大距离为 2 000 m；采用 1 对单模光纤传输时，最大距离为 40 000m。

4.1.3 1 Gbps 以太网标准

1 Gbps 以太网（Gigabit Ethernet，千兆位以太网）与以太网相似，采用同样的 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波监听多路访问/冲突检测）协议，同样的帧格式，是 IEEE 802.3 以太网标准的扩展，传输速度可达 1000 Mbps（即 1 Gbps）。有关千兆位以太网标准有两个，一是 IEEE 802.3z（定义 1000Base-LX、1000Base-SX、1000Base-LH、1000Base-ZX 和 1000Base-CX），二是 IEEE 802.3ab（定义 1000Base-T），分别用于在光纤和非屏蔽线缆上传输千兆位信号。

1. 1000Base-LX 标准

1000Base-LX 使用长波激光作为信号源，波长为 1270～1355 nm（一般为 1300 nm），既适用于多模光纤，也适用于单模光纤，主要应用在园区网络的骨干连接。1000Base-LX 可使用的光纤规格如下：

- 62.5 μm 多模光纤（Multi Mode Fiber，MMF）
- 50 μm 多模光纤
- 9 μm 单模光纤（Single Mode Fiber，SMF）

其中，使用 62.5 μm 多模光纤，全双工模式下最长有效距离为 550 m；使用 50 μm 多模光纤，全双工模式下最长有效距离为 1550 m；使用单模光纤时，全双工模式下的最长有效距离为 5～10 km。图 4-2 所示为 4 芯 50 μm 多模光纤。

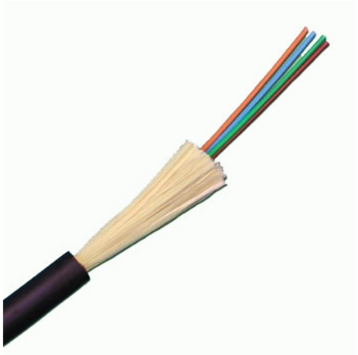


图 4-2　多模光纤

> **提示** 多模光纤和单模光纤从外观上很难区分。不过，通常情况下，单模光纤外套多为黄色，而多模光纤外套多为橙色。

2. 1000Base-SX 标准

1000Base-SX 使用短波激光作为信号源，波长为 770～860 nm（一般为 800 nm），仅适用于多模光纤，而不支持单模光纤，主要应用在建筑物内的网络骨干连接。1000Base-SX 可使用的光纤规格如下。

- 62.5 μm 多模光纤
- 50 μm 多模光纤

使用 62.5 μm 多模光纤，全双工模式下的最长传输距离为 275 m；使用 50 μm 多模光纤，全双工模式下最长有效距离为 550 m。

3. 1000Base-LH 标准

1000Base-LH 使用长波激光作为信号源，波长为 1270～1355 nm（一般为 1300 nm），既适用于多模光纤，也适用于单模光纤，主要应用在园区网络的骨干连接。1000Base-LH 可使用的光纤规格如下。

- 62.5 μm 多模光纤
- 50 μm 多模光纤
- 9 μm 单模光纤

其中，使用 62.5 μm 多模光纤，全双工模式下最长有效距离为 550 m；使用 50 μm 多模光纤，全双工模式下最长有效距离为 1550 m；使用 9 μm 单模光纤时，全双工模式下的最长有效距离为 10 km。

4. 1000Base-ZX 标准

1000Base-ZX 使用长波激光作为信号源，波长为 1550 nm，只适用于单模光纤，主要应用在园区网络的骨干连接。

使用 9 μm 单模光纤，全双工模式下最长有效距离为 70～100 km。

5. 1000Base-T 标准

1000Base-T 用于超五类及其以上屏蔽或非屏蔽双绞线，传输距离为 100 m，既可应用于服务器和高速工作站的网络接入，也可作为建筑物内的千兆位骨干连接。与 100Base-TX 不同，1000Base-T 在传输中将用到全部的 4 对线，在每个线对上传输 250 Mbps，并工作在全双工模式。图 4-3 所示为六类屏蔽双绞线，图 4-4 所示为六类非屏蔽双绞线。

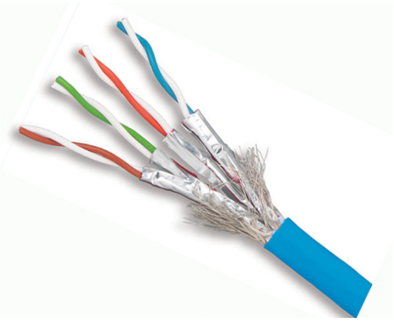


图 4-3　六类屏蔽双绞线

图 4-4　六类非屏蔽双绞线

提示：由于 100Base-TX 只用到 2 对线，因此，只要 1、2、3、6 线畅通即可进行通信。而 1000Base-T 需要使用到全部 4 对线，因此，所有线缆必须全部畅通才行。

1000Base-T 为以太网/快速以太网络向高速网络的移植提供了一种简单、廉价的方案，具有以下特点。

- 1000Base-T 完全兼容原有的以太网和快速以太网，实现 10/100/1000 Mbps 自适应连

接，为现有的以 100 Mbps 为基础的网络提供平滑的过渡。

- 1000Base-T 具有更高的性价比。当传输距离小于 100 m 时，1000Base-T 显然比 1000Base-LX/SX 更具价格优势，既无需敷设昂贵的光纤，也无需购置昂贵的光纤模块。
- 1000Base-T 可以保留以太网的设备和设施投资，其中包括在五类线设施上的已有投资。在墙体、天花板和架空地板中进行线缆更新是既费时而又需要大量投资的工作，而 1000Base-T 则不需要进行这些工作。

提·示 在超五类和六类双绞线上可以轻而易举地实现 1000Base-T，但在五类双绞线上则需要借助于特殊的设备，因此不建议在五类双绞线上进行升级。

6. 1000Base-CX 标准

采用 150Ω 平衡屏蔽双绞线（STP）作为传输介质（连接器为 DB-9），传输距离最长仅为 25m，数据编码方法采用 8B/10B，适用于数据中心设备间（如交换机之间的连接，尤其适用于主干交换机和主服务器之间的短距离连接），或者堆叠设备间的短距离互连，但不适用于数据中心与配线架的连接。

IEEE 802.3z 和 IEEE 802.3ab 标准定义的 1000 Mbps 网络的传输介质与有效传输距离，如表 4-1 所示。

表 4-1 1000 Mbps 网络传输介质与有效传输距离

标 准	波长（nm）	光纤类型	芯径（Micron）	模式带宽（MHz/km）	有效传输距离（m）
1000Base-SX	850	MMF	62.5	160	220
			62.5	200	275
			50.0	400	500
			50.0	500	550
1000Base-LX/LH	1310	MMF	62.5	500	550
			50.0	400	550
			50.0	500	550
		SMF	9/10	N/A	10 000
1000Base-ZX	1550	SMF	9/10	N/A	70 000～100 000
1000Base-T	超五类以上屏蔽或非屏蔽双绞线				100
1000Base-CX	超五类以上屏蔽双绞线				25

4.1.4 10 Gbps 以太网标准

IEEE 定义 10 Gbps 以太网（10 Gigabit Ethernet，万兆以太网）的标准为 802.3ae、802.3ak、802.3an、802.3aq 和 802.3ap。其中，802.3ae 规定了 10GBase-LR、10GBase-SR 、10GBase-ER、10GBase-LX4、10GBase-EW、10GBase-LW 和 10GBase-SW 等多种类型。802.3ak 规定了 10GBase-CX4，802.3an 规定了 10GBase-T，802.3aq 规定了 10GBase-LRM，802.ap 规定了 10GBase-KX4 和 10GBase-KR。

1. 10GBase-SR 标准

10GBase-SR（Short Range，即短距离）基于多模光纤，采用 850nm 短波，62.5 MMF 光纤下的传输距离约为 30 m，50 MMF 光纤下的有效传输距离为 300 m。10GBase-SR 具有最低成本、最低电源消耗和最小的光纤模块等优势。图 4-5 所示为 Cisco 10GBase-SR 模块。

2. 10GBase-LR 标准

10GBase-LR（Long Range，即长距离）使用单模光纤（基于 G.652 的 SMF），采用 1 310 nm 波长，有效传输距离为 2m～10 km。图 4-6 所示为 Cisco 10GBase-LR 模块。

图 4-5 Cisco 10GBase-SR 模块

图 4-6 Cisco 10GBase-LR 模块

3. 10GBase-LRM 标准

10GBASE-LRM（Long Range Multimode，即长度延伸多点模式）标准对应较早发布的 IEEE 802.3aq 标准。该标准使用 1310 nm 波长激光，适用于 50μm 和 62.5 μm 多模光纤，最远传输距离为 220 m，最小传输距离为 0.5 m。虽然在连接长度方面，不如早先的 10GBase-LX4 规范，但是它的光纤模块比 10GBase-LX4 规范光纤模块具有更低的成本和更低的电源消耗。

4. 10GBase-ER 标准

10Gbase-ER（Extended Range，即超长距离）使用单模光纤（基于 G.652 的 SMF），采用 1 550 nm 波长，有效传输距离为 2m～40 km。

5. 10GBase-ZR 标准

10GBase-ZR 在单模式光纤下支持大概 80 km 的链路长度。虽然它也是一个 10 Gbps 的以太网规格，不过，它是建立在 Cisco 光学标准上，而不是 IEEE 10 Gb 以太网的一部分。10GBase-ZR 适用单模光纤，使用 1 550 nm 的激光。图 4-7 所示为 Cisco 10GBase-ZR 模块。

6. 10GBase-LX4 标准

10Gbase-LX4 适用于多模光纤和单模光纤，使用 1310 nm 波长激光。采用多模光纤时，有效传输距离为 2m～300 m；采用单模光纤时，有效传输距离为 2m～10 km。由于 10GBase-LX4 标准采用了 4 路激光光源，所以在成本、光纤线径和电源成本方面较 10GBase-LRM 标准有不

足之处。图 4-8 所示为 Cisco 10GBase-LX4 模块。

图 4-7　Cisco 10GBase-SR 模块

图 4-8　Cisco 10GBase-LX4 模块

7.　10GBase-CX4 标准

10GBase-CX4 标准采用铜缆，利用 4 对发送器和 4 对接收器，以差分方式运行在双轴电缆上，每对收发完成 2.5 Gbps 速率的传送，有效传输距离为 15 m。由于传输距离太短，因此，只能用于网络中心机房内，实现核心层交换机与服务器之间，以及核心层交换机与汇聚层交换机之间的连接。目前，该标准已经基本被 10Base-T 标准所取代。图 4-9 所示为 Cisco 10GBase-CX4 模块。

8.　10GBase-T 标准

10GBase-T 标准是运行在双绞线上的万兆位以太网标准，使基于铜缆的楼宇万兆位以太网实施成为可能。10GBase-T 使用 650MHz 版本 RJ-45 连接器，在 Cat 6 双绞线上最长有效传输距离为 55m，在 Cat 6a 双绞线上可以达到 100m。图 4-10 所示为 Cisco 10GBase-T 模块。

图 4-9　10Gbase-CX4 模块

图 4-10　10GBase-T 万兆位以太网模块

表 4-2 所示为 10 Gbps 以太网支持的传输介质及其最远有效传输距离。

9.　10GBase-KX4 和 10GBase-KR 标准

10GBase-KX4 和 10GBase-KR 标准对应较早的 802.3ap 标准，主要用于背板应用，如刀片服务器、路由器和交换机的集群线路卡，所以又称为“背板以太网”。

表 4-2　10 Gbps 以太网有效传输距离

	波长（nm）	线缆类型	芯径（μm）	模式带宽（MHz/km）	有效传输距离（m）
10GBase-CX4	-	CX4（铜缆）	-	-	15
10GBase-T	-	CAT6A/CAT7（铜缆）	-	-	100
10GBase-SR	850	MMF	62.5	160	2～26
			62.5	200(OM1)	2～33
			50.0	400	2～66
			50.0	500(OM2)	2～82
			50.0	2 000(OM3)	2～300
			50.0	4700(OM4)	2～400
10GBase-LX4	1 310	MMF	62.5	500	2～300
			50.0	400	2～240
			50.0	500	2～300
		SMF	10.0	-	2～10 000
10GBase-LR	1 310	SMF	G.652	-	2～10 000
10GBase-ER	1 550	SMF	G.652	-	2～40 000
10GBase-LRM	1 310	MMF	62.5	500	0.5～220
			50	400	0.5～100
			50	500	0.5～220
		SMF	G.652	-	0.5～300
10GBbase-ZR	1 550	SMF	任何 SMF 类型	-	2～80 000
10GBase-LW	1 310	SMF	G.652	-	2～10 000
10GBase-SW	850	MMF	G.652	500	2～300
10GBase-EW	1 550	SMF	G.652	-	2～40 000

万兆背板包括并行和串行两种版本。并行版，即 10GBase-KX4 标准，是背板的通用设计，将万兆信号拆分为 4 条通道，每条通道的带宽都是 3.125 Gb/s。串行版，即 10Base-KR 标准，只定义了一条通道，采用 64/66B 编码方式实现 10 Gb/s 高速传输。在 10GBase-KR 规范中，为了防止信号在较高的频率水平下发生衰减，背板本身的性能需要更高，而且可以在更大的频率范围内保持信号的质量。

10.　10GBase- SW/LW/EW/ZW 标准

10GBase-W 系列是广域网标准，包括 10GBase-SW、10GBase-LW、10GBase-EW 和 10GBase-ZW。其中，10GBase-SW 使用多模光纤，采用 850 nm 波长，传输距离为 2～300 m。10GBase-LW 使用单模光纤，采用 1310 nm 波长，传输距离为 2～10 km。10GBase-EW 使用单模光纤，采用 1 550 nm 波长，传输距离为 2～40 km。10GBase-ZW 使用单模光纤，采用 1 550 nm 波长，传输距离为 2～80 km。

4.1.5　40/100 Gbps 以太网标准

IEEE 802.3ba 标准于 2010 年 6 月获得通过，用于规范 40/100 Gbps 以太网，同时确立了通过主干网络、铜缆布线、多模光缆和单模光缆通信的物理层规范。该标准支持 40 Gbps 速率下 100 m 多模光纤传输、10 m 铜线传输和 1 m 背板传输。在 100 Gbps 领域，支持 10 km、40 km

单模光纤传输、100 m 多模光纤传输、10 m 铜线传输。40 Gbps 主要面向服务器，而 100 Gbps 则面向网络汇聚和骨干，用于解决数据中心、运营商网络和其他流量密集高性能计算环境中数量越来越多的应用的宽带需求。

40 GE 以太网标准包括：

40GE Base-LR4，基于单模光纤（SMF），传输距离不小于 10 km。

40GE Base-SR4，基于 OM3 多模光纤（MMF），传输距离不小于 100 m。

40GE Base-CR4，基于铜缆，传输距离不小于 10 m。

40GE Base-KR4，基于背板，传输距离不小于 1 m。

如图 4-11 所示为 Cisco 40GBASE QSFP 模块。

图 4-11　Cisco 40GBASE QSFP 模块

100 GE 以太网标准包括：

100 GE Base-ER4，基于单模光纤（SMF），传输距离不小于 40 km。

100 GE Base-LR4，基于单模光纤（SMF），传输距离不小于 10 km。

100 GE Base-SR10，基于 OM3 多模光纤（MMF），传输距离不小于 100 m。

100 GE Base-CR10，基于铜缆，传输距离不小于 10 m。

表 4-3　40GE/100GE 接口类型及定义

接口类型	定　义
40 GE-聚合速率	41.25 Gbit/s 采用 64B/66B 编码
1 m 背板	4×10 Gbit/s 基于 10 Gbit/s Back-KR
1 m 铜缆	4×10 Gbit/s 基于 10 Gbit/s Back-KR
100 m MMF(OM3)	4×10 Gbit/s，每个方向 4 根光纤
10 km SMF(LR4)	4×10 Gbit/s，1.3 μm CWDM
100 GE-聚合速率	103.125 Gbit/s 采用 64B/66B 编码
10 m 铜缆	10×10 Gbit/s 基于 10 Gbit/s Back-KR
100 m MMF(OM3)	10×10 Gbit/s，每个方向 10 根光纤
10 km SMF(LR4)	4×25 Gbit/s，1.3 μm LAN CWD(800 GHz)
40 km SMF(ER4)	4×25 Gbit/s，1.3 μm LAN CWD(800 GHz)

4.2　交换机端口类型

交换机的功能就是用于连接其他网络设备（如交换机、路由器、网络防火墙等），以及网

络终端设备（如计算机、网络打印机、IP 电话机、网络摄像头等），从而实现相互之间的通信，构建局域网络。因此，交换机必须都拥有大量的端口。由于网络环境和网络需求非常复杂，所以交换机也就不得不拥有多种类型的端口。大致可以将交换机端口分为 4 种类型，即光纤端口、双绞线端口、插槽和复用端口。

4.2.1 光纤端口

光纤在局域网络中拥有无可比拟的优势。第一，光纤的有效传输距离最远，几百米甚至几十千米都没有问题，因此被广泛应用于楼宇之间、楼层之间的连接。第二，光纤的抗电磁干扰能力强，无论多么恶劣和复杂的环境，都丝毫不受影响。第三，传输速率高，1 Gbps 甚至 10 Gbps 都可以轻松实现，最适宜高速设备之间的连接。

图 4-12 所示为 100Base-FX 光纤端口，可以实现 100 Mbps 的远程连接，适用于 62.5 μm/125 μm 或 50 μm/125 μm 多模光纤。

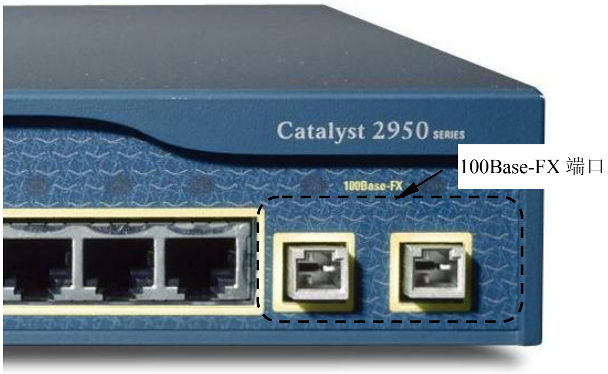


图 4-12　100Base-FX 光纤端口

图 4-13 所示为 1000Base-SX 光纤端口，可以实现 1000 Mbps 的高速远程连接，并可用于实现 Gigabit EtherChannel，适用于 62.5 μm/125 μm 或 50 μm/125 μm 多模光纤。

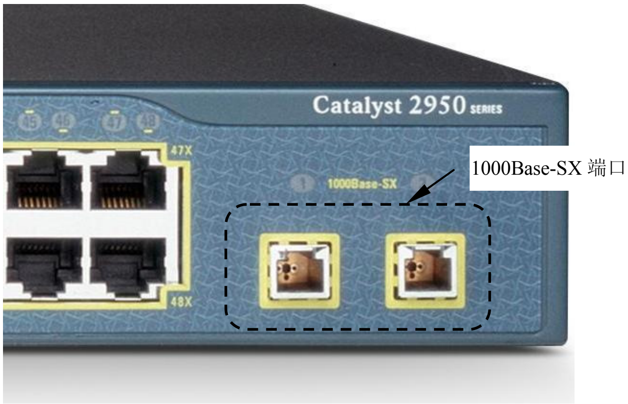


图 4-13　1000Base-SX 光纤端口

提·示 与 1000Base-T 不同，1000Base-SX、1000Base-LX/LH 和 1000Base-ZX 均不能支持自适应，不同速率和双工工作模式的端口将无法连接并通信。因此，要求相互连接的光纤端口必须拥有完全相同的传输速率和双工工作模式，既不可将 1000 Mbps 的光纤端口与 100 Mbps 的光纤端口连接在一起，也不可将全双工模式的光纤端口与半双工模式的光纤端口连接在一起，否则将导致连通性故障。

4.2.2 双绞线端口

双绞线端口是应用最多也是最廉价的端口类型。双绞线网络的优点有 4 个：一是价格低廉，这也正是其被广泛采用的原因之一；二是连接简单，将跳线两端的水晶头插入 RJ-45 端口，即可完成设备之间的连接；三是传输速率高，可以轻松实现 1000 Mbps 的高速连接；四是自适应，可以智能判断对端设备的传输速率和工作模块，自动进行协商，建立所能达到的最高的传输速率。缺点有两个，一是传输距离较短，100 Mbps 和 1000 Mbps 网络只能传输 100 m。不过，对于一般的网络连接而言，这样的距离也已经足够了。二是抗干扰能力差，要求外界环境不能有太多的电磁干扰。

图 4-14 所示为 10/100 Mbps 自适应（100Base-TX）双绞线端口，用于实现与普通计算机和网络终端的连接。该类端口要求使用五类以上的非屏蔽双绞线连接。

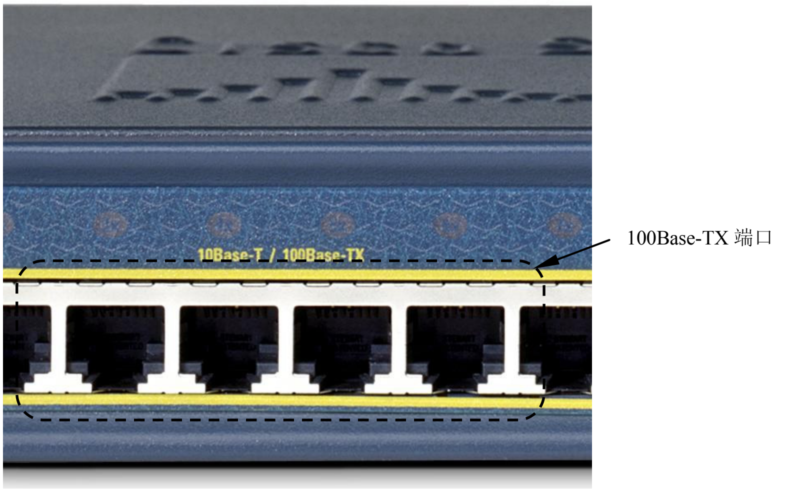


图 4-14 双绞线端口

图 4-15 所示为 10/100/1000 Mbps 自适应（1000Base-T）双绞线端口，用于实现与其他交换机（尤其是汇聚层交换机）的级联，也可用于连接小型网络中的服务器。该类端口要求使用超五类或六类非屏蔽双绞线连接。

提·示 100Base-TX 和 1000Base-T 端口在外观上没有什么分别，因此必须借助交换机上的端口标记才能区分。另外，100Base-TX 和 1000Base-T 端口均可用于创建 EtherChannel，成倍提高连接带宽，并实现链接冗余和负载均衡。

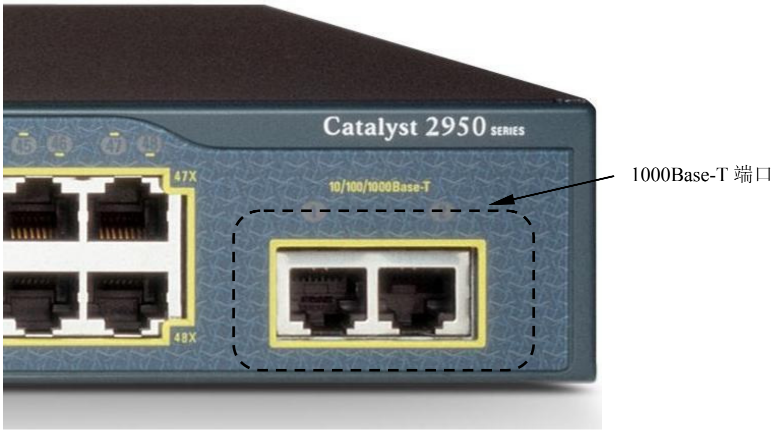


图 4-15　1000Base-T 端口

4.2.3 1GE 模块与插槽

1GE 模块与插槽的类型主要包括两种，即 GBIC 和 SFP。

1. GBIC 模块与插槽

GBIC（Gigastack Gigabit Interface Converter）是一个通用的、低成本的千兆位以太网连接标准，用于提供交换机与其他设备之间的高速（1000 Mbps）连接。借助不同的 GBIC 模块，既可建立高密度端口的叠堆，又可实现与服务器，或者远程主干网络的高速连接，因此具有非常大的灵活性。图 4-16 所示为 GBIC 插槽。

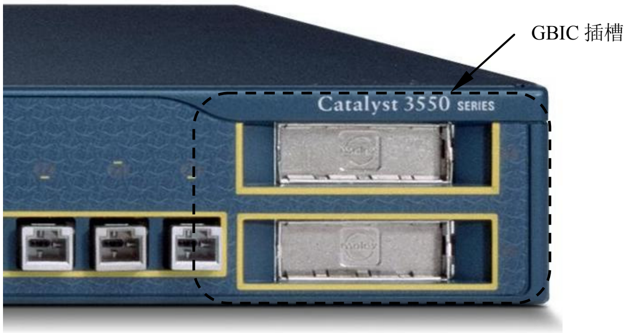


图 4-16　GBIC 插槽

GBIC 模块分为四种，一是 1000Base-T GBIC 模块（如图 4-17 所示），适用于超五类或六类双绞线，最长传输距离为 100 m；二是 1000Base-SX GBIC 模块（如图 4-18 所示），适用于多模多纤（MMF），最长传输距离为 500 m；三是 1000Base-LX/LH GBIC 模块，适用于单模光纤（SMF），最长传输距离为 10 km；四是 1000Base-ZX GBIC，适用于长波单模光纤，最长传输距离为 70～100 km。由此可见，只需更换 GBIC 模块，交换机就可以适用于各种传输介质和网络环境，为用户提供高速连接和应用。

图 4-17　1000Base-T GBIC 模块

图 4-18　1000Base-SX GBIC 模块

2.　SFP 模块与插槽

SFP（Small Form-factor Pluggable，小型可插拔）可以简单地理解为 GBIC 的升级版本，同样能够提供高达 1000 Mbps 的连接。事实上，SFP 已经取代 GBIC 成为新的千兆位接口标准，而 GBIC 则基本上已经退出了市场。

SFP 插槽（如图 4-19 所示）所占用的位置比 GBIC 模块减少一半，因此可以在面积相同的面板上设置多一倍的端口数量。由于 SFP 模块在功能上与 GBIC 基本一致，只是体积“MINI”（微型）化，因此也被称为小型化 GBIC（Mini-GBIC）。

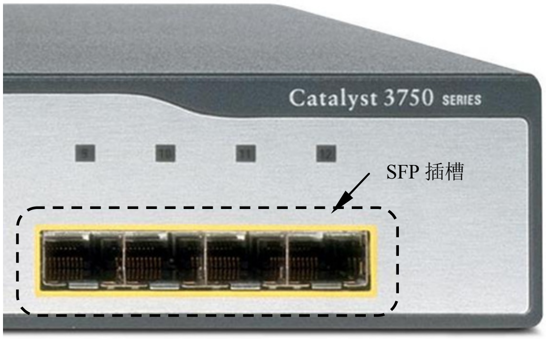


图 4-19　SFP 插槽

SFP 模块的类型与 GBIC 非常相似，也可分别应用于双绞线（如图 4-20 所示）、多模光纤和单模光纤（如图 4-21 所示），从而使网络连接变得更加灵活，适应更为复杂的网络环境。SFP 的类型也与 GBIC 一样，主要分为 1000 Base-T、1000Base-SX、1000Base-LH/LX 和 1000Base-ZX 等 4 种类型。

图 4-20　1000Base-T SFP 模块

图 4-21　1000Base-SX SFP 模块

4.2.4 10GE 模块与插槽

10 Gbps 端口是当今速度最快、价格最昂贵的端口之一，因此，10 Gbps 端口通常用于实现重点业务的汇聚层交换机与核心层交换机之间的连接。10 Gbps 端口通常借助于不同标准的插槽和模块实现，主要包括 XENPAK、X2、XFP 和 SFP+等 4 种。

1. XENPAK

XENPAK 是面向万兆位以太网的第一代模块。根据 XENPAK 多方协议提议，收发器模块采用了 XAUI 接口。其中 1310 nm 串行收发器，传输距离可达 10 km，使用了直接调制激光器技术，不再需要传统的调制器、冷却器或复杂的光复用器。这种模块具有良好的抗 EMI 和散热性能，每个线路卡最多可实现 8 个端口的高密度配置，其面板热插拔特性使 4 种物理层介质设备收发器都能实现即插即用。图 4-22 所示为提供两个 XENPAK 插槽的 Catalyst 6500 系列管理引擎模块。

图 4-22　XENPAK 插槽

图 4-23 所示为 XENPAK 光纤模块。

图 4-23　XENPAK 光纤模块

2. X2

X2 和 XPAK 是 XENPAK 模块的直接改进版，体积缩小了 40%，光接口、电接口都与原来保持一致。X2 模块目前应用最普遍，Cisco Catalyst 3560-E、Catalyst 3750-E 和 Catalyst 4900 系列，以及 Catalyst 4500-E 和 Catalyst 6500-E 系列中，X2 插槽都被大量应用。图 4-24 所示为 X2 插槽，图 4-25 所示为 X2 万兆位光纤模块。

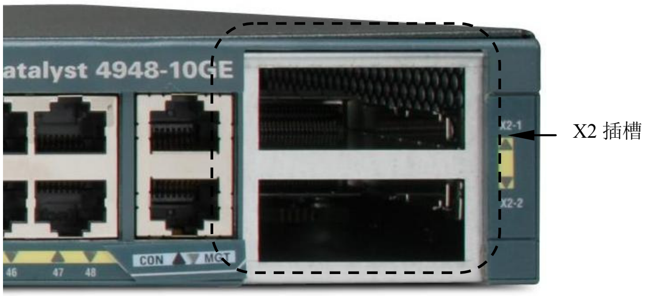


图 4-24　X2 插槽

3. XFP

XFP（10-Gigabit Small Form-factor Pluggable）支持局域网 PHY 和广域网 PHY，具有可插拔、尺寸更加小巧、价格更有竞争力等特点。因此，大多数最新的设计全都采用 XFP 模块，这是因为它物理尺寸的小型化可以达到很高的端口密度。可以预见，使用 XFP 模块的产品很快会成为市场新宠。XFP 更多地被应用于路由器模块。图 4-26 所示为 XFP 万兆位模块和插槽。

图 4-25　X2 光纤模块

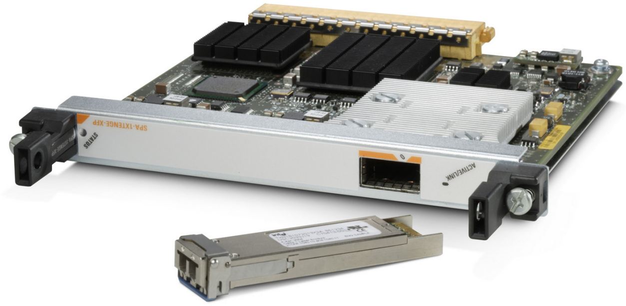


图 4-26　XFP 插槽和模块

4. SFP+

SFP+（Small Form-factor Pluggable Plus）是用于 10 Gbps 以太网的可插拔模块尺寸规格，最多可提供 11.1 Gbps 的速率。

SFP+得名于 SFP，并与 SFP 模块采用同样的物理尺寸，因此能够与旧的 SFP 模块在同样的插槽中工作。SFP+模块比 XFP 更小，由此也把每个线卡的密度从 XFP 的 16 个提高到至少 24 个。

SFP+模块可用于替代目前的 XFP、XENPAK 和 X2 等万兆位模块。SFP+相对于这些万兆位模块，其主要优势如下：

- 体积优势。SFP+体积与 SFP 一样，相对于其他类型的万兆位模块，体积大大减小，有利于在更小的体积上，实现更多的万兆位端口。
- 成本优势。由于 SFP+模块相对于 XFP 模块，删除了 CDR（时钟数据恢复模块），因此，在成本上会有降低。

- 电源功耗降低。XENPAK 的功耗最低为 9 W，X2 的功耗为 4 W，XFP 的功耗为 2.5～3.5 W，而 SFP+的功耗只有 1 W，从而无需专门的散热部件散热，降低了整板的功耗及对散热的要求。

图 4-27 所示为 Catalyst 2960-S 提供的 SFP+插槽，图 4-28 所示为 SFP+模块。

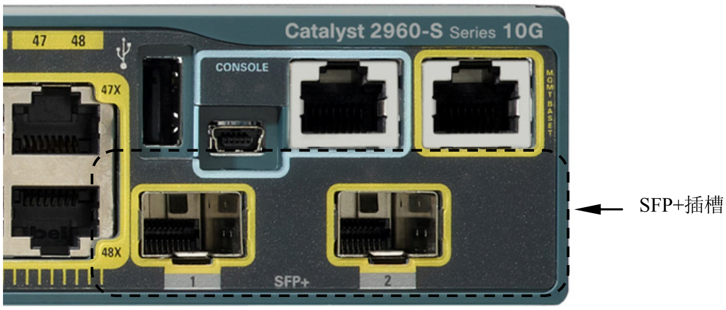


图 4-27　SFP+插槽

图 4-28　SFP+模块

4.2.5 40GE 模块与插槽

QSFP（Quad Small Form-Factor Pluggable，四通道小型可插拔)）是用于 40 Gbps 以太网的最新可插拔模块尺寸规格，用于满足市场对更高密度的高速可插拔解决方案的需求。4 通道的可插拔接口传输速率达到了 40 Gbps，很多 XFP 中成熟的关键技术都应用于该产品设计中。

QSFP 可在 XFP 相同的端口体积下，以每通道 10 Gbps 的速度支持四个通道的数据传输，所以 QSFP 的密度可以达到 XFP 产品的 4 倍，SFP+产品的 3 倍。具有 4 通道且密度比 CX4 高的 QSFP 接口已经被 InfiniBand 标准所采用。

图 4-29 所示为 Cisco 48p 1/10G-T and 4p 40G QSFP+ Nexus 9000 线卡提供的 QSFP 插槽，图 4-30 所示为 QSFP 模块。

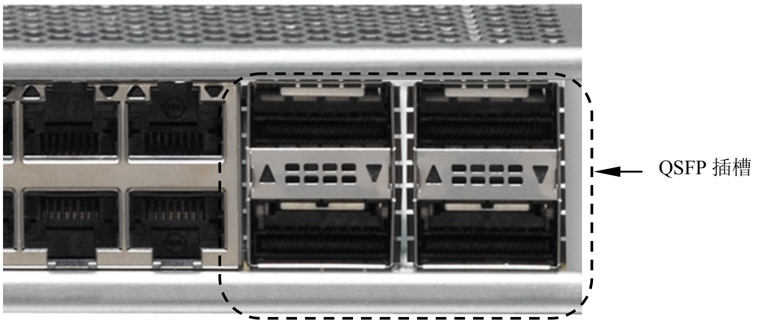


图 4-29　QSFP 插槽

图 4-30　QSFP 模块

4.2.6 复用端口

有些级联端口虽然是独立的、端口类型不同的两个端口，但这两个端口中只能使用其中的一个，不能同时用于连接设备。这类端口称之为复用端口，设计的目的是为了提高网络设备的可用性。

图 4-31 所示为 100Base-FX 与 1000Base-X SFP 复用端口。由于光纤链路的两端必须采用相同的传输速率和工作模式，因此该复用端口可用于连接 100 Mbps 或 1000 Mbps 光纤网络。

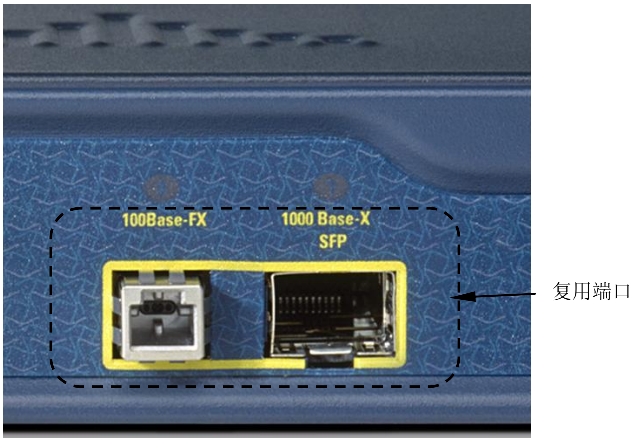


图 4-31　100Base-FX 与 1000Base-X SFP 复用端口

图 4-32 所示为 1000Base-T 与 1000Base-X SFP 复用端口。当采用双绞线与其他交换机或高端计算机设备短程连接时，直接使用 1000Base-T 端口就行了。若欲实现与汇聚层交换机、甚至核心层交换机的远程连接时，则插入相应的 SFP 模块即可。

图 4-32　1000Base-T 与 1000Base-X SFP 共用端口

4.2.7 10GE 转换模块

1. TwinGig

TwinGig 模块用于 Cisco Catalyst 3560-E/3750-E 系列交换机。借助 Cisco TwinGig 转换模块（如图 4-33 所示），可以将 10 Gb Ethernet 插槽转换成 2 个 SFP 插槽，实现双 1000 Mbps 端口连接。

图 4-34 所示为借助 Cisco TwinGig 转换模块，将 2 个 SFP 模块连接至 1 个 10 Gbps 插槽。

图 4-33　TwinGig 转换模块

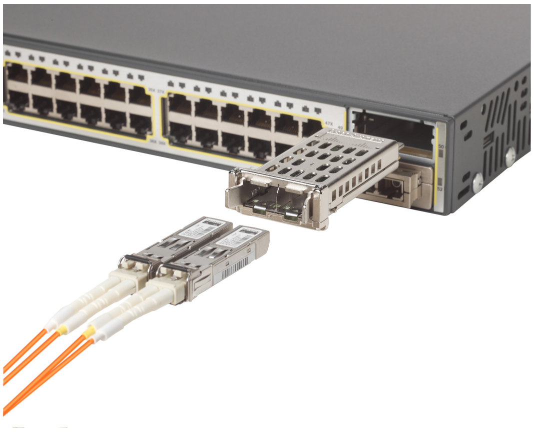


图 4-34　TwinGig 转换模块连接

2. OneX

OneX 转换模块是一个可热插拔的 10 Gb Ethernet X2 插槽模块，用于实现 10 Gb X2 接口与单 10 Gb SFP+接口的转换，支持 Catalyst 3750/4500/4900/6500 等多个交换机平台。如图 4-35 所示为 OneX 转换模块，如图 4-36 所示为 OneX 转换模块连接方式。

图 4-35 OneX 转换模块

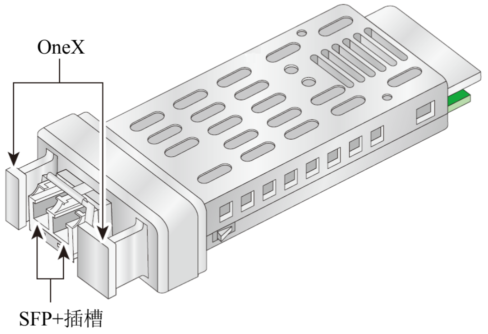


图 4-36 OneX 转换模块连接

4.3 跳线与使用

网络设备之间，以及网络设备与计算机、终端设备之间的连接，都是借助跳线来完成的。跳线就像一条纽带，将相关的设备连接在一起。然后，通过综合布线系统，实现所有设备的互连互通。

4.3.1 双绞线跳线

双绞线跳线用于连接双绞线端口。双绞线跳线比较简单，两端均为统一的标准 RJ-45 端口，如图 4-37 所示。

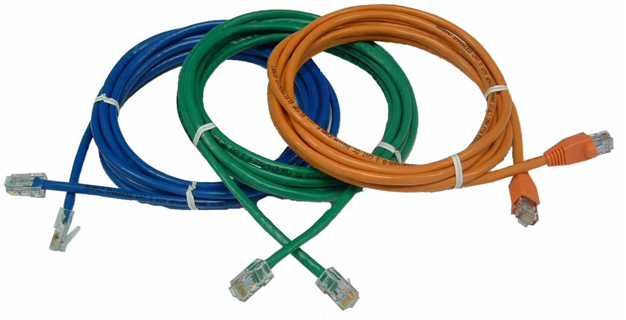


图 4-37 双绞线跳线

100 Mbps 端口之间的连接，可以使用超五类非屏蔽双绞线制作的跳线；若欲连接的是 1000 Mbps 端口，就应当使用专业的六类非屏蔽双绞线跳线，以避免由于跳线的电磁性能不达

标，而导致网络通信质量的下降。

只需将跳线两端的水晶头分别插入网络设备的 RJ-45 端口，即可将其连接在一起。图 4-38 所示为将跳线的一端连接至交换机的 1000Base-T 端口，图 4-39 所示为将跳线的另一端连接至 GBIC 的 RJ-45 端口。

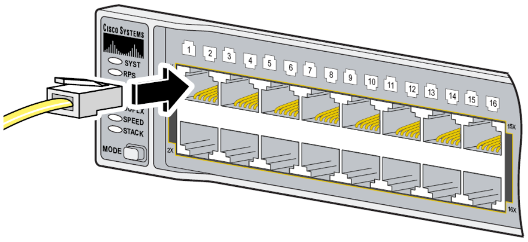


图 4-38　连接至 1000Base-T 端口

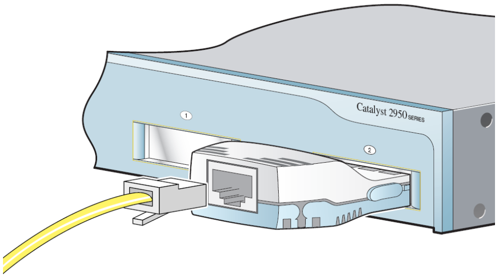


图 4-39　连接至 GBIC 插槽

双绞线跳线有两种不同的类型，即直通线和交叉线，拥有各自不同的用途。

- 直通线。两端 RJ-45 头中的线序排列完全相同的网线，称为直通线（Straight Cable），即当一端线序从左到右依次为白橙、橙、白绿、蓝、白蓝、绿、白棕、棕时，另一端线序从左到右仍然依次为白橙、橙、白绿、蓝、白蓝、绿、白棕、棕（如图 4-40 所示）。直通线通常适用于计算机、路由器与交换机之间的连接。
- 交叉线。当使用双绞线直接连接两台计算机或连接两台集线设备时，另一端的线序应作相应的调整，即第 1、2 线和第 3、6 线对调，制作为交叉线（Crossover Cable）。例如，当一端线序从左到右依次为：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕时，另一端线序从左到右应当依次调整为白绿、绿、白橙、蓝、白蓝、橙、白棕、棕（如图 4-41 所示）。交叉线通常适用于交换机之间的连接。

图 4-40　直通线

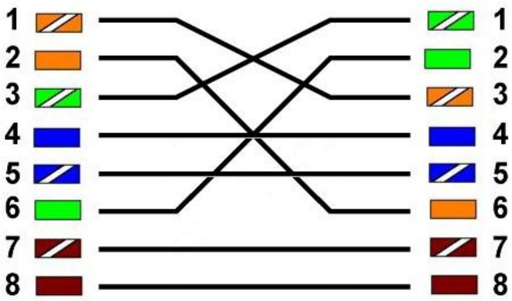


图 4-41　交叉线

提·示　交换机之间的连接（尤其是 1000Base-T 端口之间的连接）使用的双绞线跳线应当尽量使用六类成品跳线，以保证其电气性能。综合布线中使用的双绞线跳线，则应当与布线系统所采用的标准相同。即，如果布线系统采用超五类布线系统，那么，就应当采用超五类跳线；如果布线系统采用六类布线系统，那么，就应当采用六类跳线。

4.3.2 光纤跳线

光纤跳线的作用与双绞线跳线类似，也是用于连接网络设备和计算机，实现彼此之间的相互通信。光纤跳线中间是 3～5 m 左右的光纤，其两端是光纤连接器（如图 4-42 所示），分别连接两端设备的光纤端口。由于光纤端口的种类比较多，因此只有选择与之相适应的连接器，才能实现匹配与连接。

图 4-42　光纤跳线

1. LC 型光纤连接器

LC 型连接器（如图 4-43 所示）采用操作方便的模块化插孔（RJ）闩锁机理制成，采用的插针和套筒的尺寸为 1.25 mm，由于占用的空间很小，因此可以有效地提高光纤端口的密度。SFP 模块、SFP+模块、XFP 模块和 QSFP 模块均采用 LC 型光纤连接器。

图 4-44 所示为已经插入一根光纤跳线的 SFP 模块。当然，若欲实现设备之间的正常连接，必须使用一对光纤连接才行。

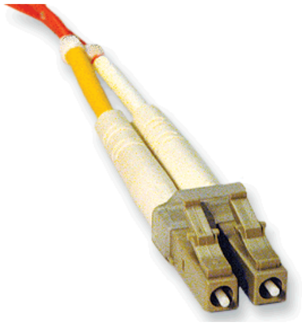


图 4-43　LC 型连接器

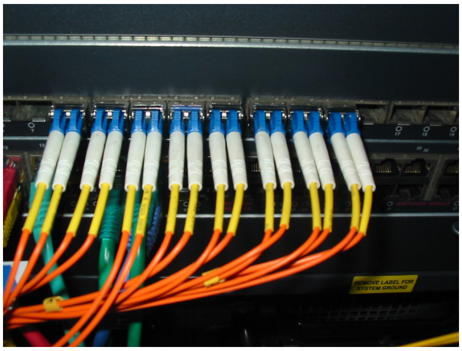


图 4-44　LC 型连接器插入 SFP 模块

2. SC 型光纤连接器

SC 型光纤连接器（如图 4-45 所示）外壳呈矩形，采用插针与耦合套筒结构。紧固方式是采用插拔销闩式，无需旋转。该类连接器价格低廉，插拔操作方便，介入损耗波动小，抗压强度较高，安装密度高。GBIC 模块、X2 模块、XENPAK 模块和 100Base-FX 端口使用的都是 SC 型光纤连接器。

图 4-46 所示为 SC 型光纤连接器连接至机箱式交换机中的 GBIC 模块。

图 4-45　SC 型光纤连接器

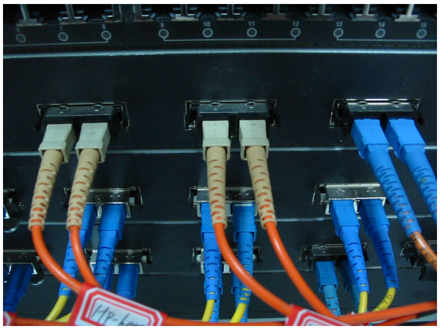


图 4-46　SC 型连接器插入 GBIC 模块

3.　ST 型光纤连接器

ST 型光纤连接器（如图 4-47 所示）外壳呈圆形，所采用的插针与藕合套筒的结构尺寸与 FC 型完全相同，其中插针的端面多采用 PC 或 APC 型研磨方式；紧固方式为螺丝扣。此类连接器适用于各种光纤网络，操作简便，且具有良好的互换性。

ST 型光纤连接器很少用于连接网络设备，而是经常被用于实现与光纤配线架的连接，如图 4-48 所示。因此，若欲将安装有 GBIC 模块的交换机连接至远程的网络骨干，就必须选择一端为 ST 型连接器，另一端为 SC 型连接器的光纤跳线。

图 4-47　ST 型连接器

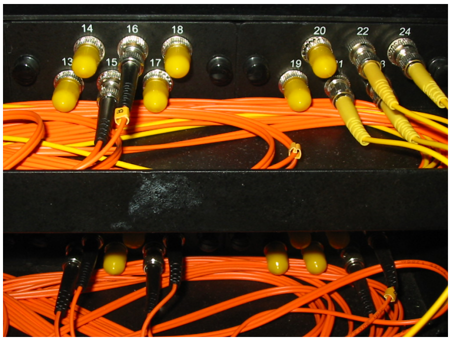


图 4-48　ST 型连接器与光纤配成架的连接

同样，若欲实现 GBIC 模块与 SFP 模块的连接，就必须选择一端为 SC 型连接器，另一端为 LC 型连接器的光纤跳线。

> **提示**　除光纤连接器必须与所连接的光纤端口相匹配外，光纤跳线也必须与所连接光纤端口或光纤模块所支持的传输介质相一致。使用多模光纤跳线连接多模光纤模块或端口的结果，只能是导致端口间无法通信。

4.　MT-RJ 型光纤连接器

MT-RJ 型光纤连接器（如图 4-49 所示）带有与 RJ-45 型 LAN 电连接器相同的闩锁机构，通过安装于小型套管两侧的导向销对准光纤，为便与光纤收发机相连，连接器端面光纤为双芯（间隔 0.75 mm）排列设计，是主要用于数据传输的高密度光连接器。

FC型连接器（如图4-50所示）最早是由日本NTT研制的。FC是Ferrule Connector的缩写，表明其外部加强方式是采用金属套，紧固方式为螺丝扣。

图4-49 MT-RJ型连接器

图4-50 FC型光纤连接器

4.3.3 光纤跳线与光纤端口

光纤跳线分为单模光纤和多模光纤。交换机光纤端口、跳线都必须与综合布线时使用的光纤类型相一致，也就是说，如果综合布线时使用的是多模光纤，那么交换机的光纤端口就必须执行1000Base-SX标准或10GBase-SR标准、10GBase-LX4标准、10GBase-LRM标准，也必须使用多模光纤跳线；如果综合布线时使用的是单模光纤，那么交换机的光纤端口就必须执行1000Base-LX/LH标准或10GBase-LR标准、10GBase-ER标准、10GBase-ZR标准，也必须使用单模光纤跳线。

需要注意的是，多模光纤有两种类型，即62.5/125 μm和50/125 μm。虽然交换机的光纤端口完全相同，而且两者也都执行1000Base-SX标准或10GBase-SR标准、10GBase-LX4标准、10GBase-LRM标准，但光纤跳线的芯径必须与光缆的芯径完全相同，否则将导致连通性故障。

另外，相互连接的光纤端口的类型必须完全相同，或者均为多模光纤端口，或者均为单模光纤端口。一端是多模光纤端口，而另一端是单模光纤端口，将无法连接在一起。

4.4 交换机的连接策略

不同性能、不同类型交换机之间的连接是有技巧的，不同的排列组合所得到的最终结果会完全不同。毫无疑问，我们必须选择性能最高的那一个。

4.4.1 不同性能交换机的连接策略

从交换机背板带宽和转发速率上看，交换机之间的性能区别很大。性能最高的交换机（通常是三层交换机）作为核心层交换机（或核心层交换机）位于网络的中心位置，用于实现整个网络中不同子网之间的数据交换；性能稍逊的交换机（可以是三层交换机）作为汇聚层交换机，用于实现某一网络子网内数据之间的交换；性能最差的交换机作为接入层交换机，用于直接连接至桌面计算机，为用户直接提供网络接入，如图4-51所示。例如，Cisco Catalyst 4506作为核心层交换机，Catalyst 3750或Catalyst 4900作为汇聚层交换机，Catalyst 2960或Catalyst 3560作为接入层交换机。

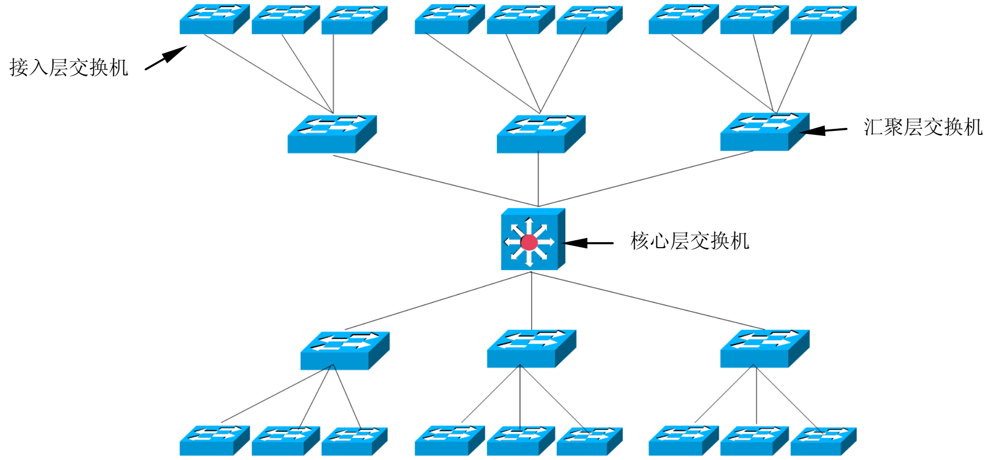


图 4-51 高性能交换机作为网络核心

4.4.2 非对称交换机的连接策略

所谓不对称网络，是指由不对称交换机构建的网络。通常情况下，高速端口用于连接其他交换机或服务器，而低速率端口则用于直接连接计算机或集线器。该连接方式同时解决了设备之间以及服务器与设备之间的连接瓶颈，充分考虑了服务器的特殊地位，通过增加服务器连接带宽，可有效地防止服务器端口拥塞的问题，同时，由于交换机之间通过高速端口通信，可使网络内所有的计算机都平等地享有对服务器的访问权限。

例如，当 Cisco Catalyst 2960 交换机相互连接时，应当使用其 1000 Mbps 端口。而与普通计算机的连接，则使用 100 Mbps 端口（如图 4-52 所示）。从而保证连接至不同交换机的计算机之间的通信畅通，不会在交换机之间产生传输瓶颈。

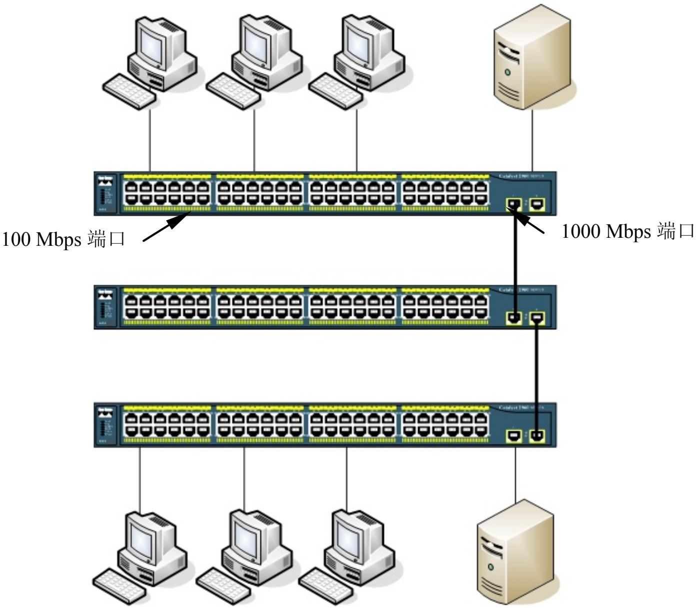


图 4-52 高速端口互连

同样，当 Cisco Catalyst 2960 接入交换机连接至 Cisco Catalyst 3750 汇聚层交换机时，也应当使用其 1000 Mbps 端口（如图 4-53 所示），以保证所连接的计算机能够实现对网络骨干的高速访问。

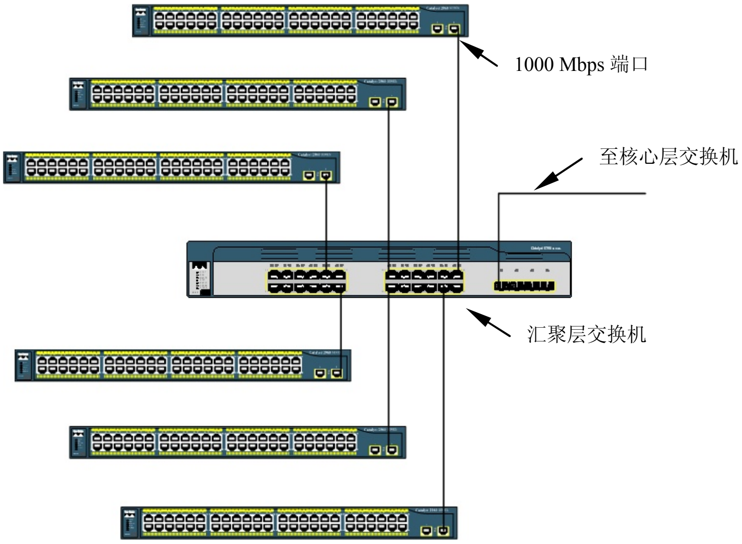


图 4-53　高速端口向上级联

4.4.3 对称交换机的连接策略

所谓对称网络，是指由对称交换机构建的网络。

对称网络的连接策略非常简单，就是选择其中一台交换机作为核心层交换机，然后将其他所有被频繁访问的设备，如其他交换机、服务器、打印机等，都连接至该交换机，而其他设备则连接至其他交换机（如图 4-54 所示）。由于所有端口只需一次交换即可实现与频繁访问的设备的连接，因此大幅度提高了网络传输效率。需要注意的是，在该拓扑结构中，对核心层交换机性能的要求比较高。如果核心层交换机的背板带宽和转发速率较差，那么将会影响整个网络的通信效率。

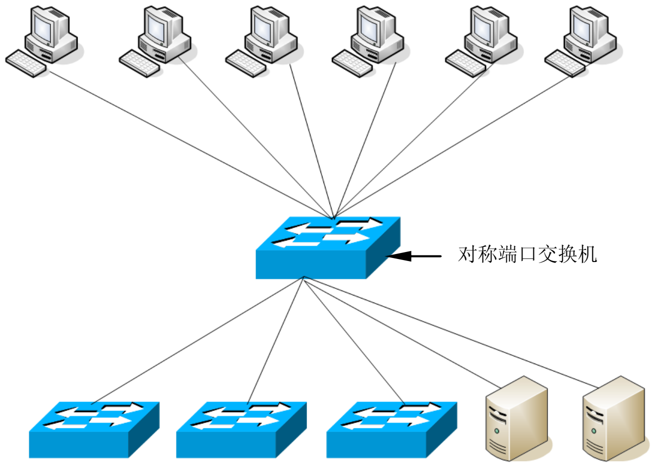


图 4-54　对称交换机之间的连接方式

4.5　交换机的连接

GBIC 模块也好，SFP 模块也好，最终都归结为采用什么样的传输介质。因此，从根本上来讲，交换机之间的连接除了使用双绞线，就是使用光纤。当然，超五类双绞线和六类双绞线只是性能上的不同，并没有使用时的差别。光纤链路则有所不同，单模光纤和多模光纤千万不能混用，否则光纤端口之间将无法通信。

4.5.1　光纤端口的连接

由于光纤端口的价格仍然非常昂贵，所以光纤主要被用于核心层交换机和汇聚层交换机之间连接，或被用于汇聚层交换机之间的级联。需要注意的是，光纤端口均没有堆叠的能力，只能被用于级联。

1.　光纤跳线的交叉连接

所有交换机的光纤端口都是 2 个，分别是一发一收。当然，光纤跳线也必须是 2 根，否则端口之间将无法进行通信。当交换机通过光纤端口级联时，必须将光纤跳线两端的收发对调，当一端接“收”时，另一端接“发”。同理，当一端接“发”时，另一端接“收”（如图 4-55 所示）。Cisco GBIC 光纤模块都标记有收发标志，左侧向内的箭头表示“收”，右侧向外的箭头表示“发”。如果光纤跳线的两端均连接“收”或“发”，则该端口的 LED 指示灯不亮，表示该连接为失败。只有当光纤端口连接成功后，LED 指示灯才转为绿色。

同样，当汇聚层交换机连接至核心层交换机时，光纤的收发端口之间也必须交叉连接，如图 4-56 所示。

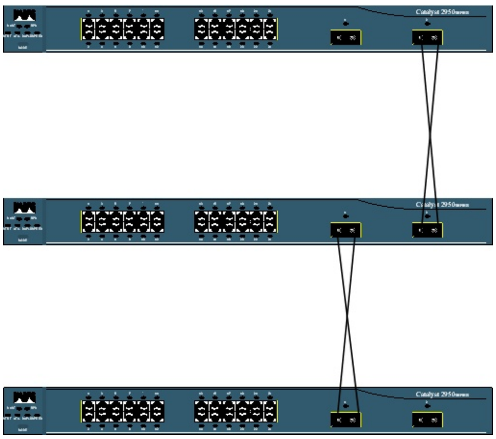


图 4-55　光纤端口的级联

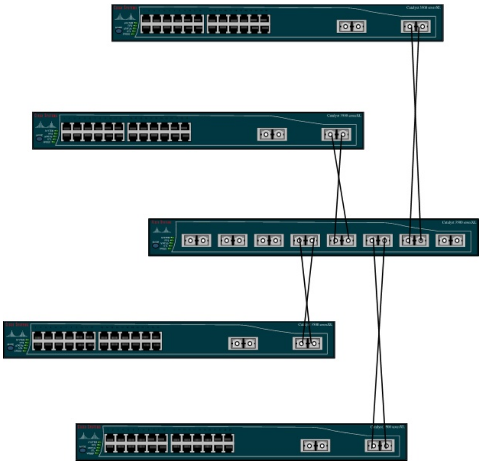


图 4-56　汇聚层交换机与接入交换机的连接

2.　光电收发器的连接

当建筑之间或楼层之间的布线采用光缆，而水平布线采用双绞线时，可以采用两种方式实现两种传输介质之间的连接。一是采用同时拥有光纤端口和 RJ-45 端口的交换机，在交换机

之间实现光电端口之间的互连；二是采用廉价的光电转换设备，一端连接光纤一端连接交换机的双绞线端口，实现光电之间的相互转换。图 4-57 所示为 SC-to-RJ-45 收发转发器。

图 4-57　光电收发转发器

相比较而言，模块化交换机的传输性能更高，而光电转换设备的价格更低。因此，应当根据网络的数据传输需要和投资额度决定采用哪种设备。需要注意的是，并非全部光纤收发器都支持全双工，部分产品只支持半双工，应当在选购时注意鉴别。另外，考虑到兼容性，建议选用相同品牌和类型的产品。

光电收发器的一端使用光纤跳线连接至光纤配线架，实现与远端光纤端口的连接；另一端使用双绞线跳线连接至交换机的 RJ-45 端口，实现与交换机上其他计算机间的连接，从而完成网络骨干的光纤传输。

当网络直径过大，已经远远超出双绞线所能支持的传输距离时，都会借助于光纤进行传输。如果网络用户数量较少，仅仅是为了实现远距离通信，对网络性能和数据传输速率没有太高要求，可以在两端均使用光电收发器＋普通 RJ-45 端口交换机的方式，从而大幅降低网络成本。网络设备的连接方式如图 4-58 所示。

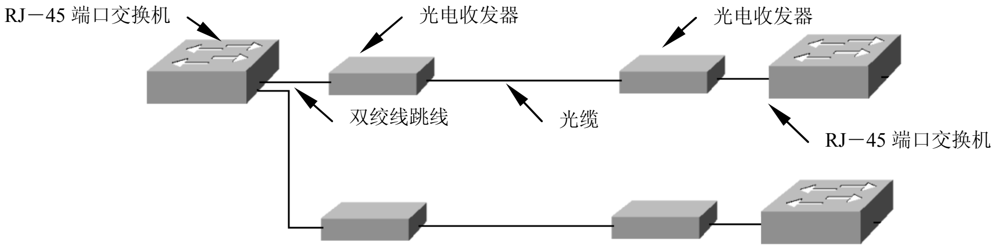


图 4-58　两端均使用光电收发转发器

如果整个网络连接有多幢建筑，而且对数据传输性能要求较高，只是某个子网无需较高的性能，则可以只在一端使用光电收发器（如图 4-59 所示），而另一端使用带有光纤接口的中心或汇聚层交换机，从而在保证整体网络性能的同时，提高网络的性价比。

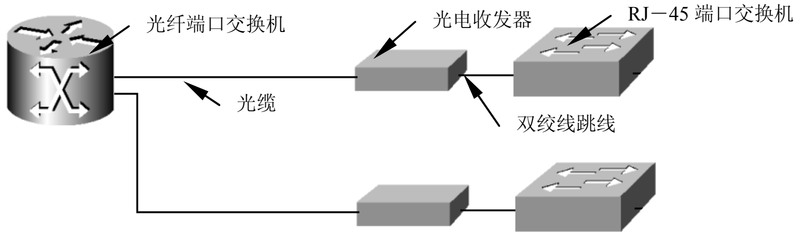


图 4-59　一端使用光电收发转发器

连接光电收发器与交换机时，应当注意以下几个方面的问题。

- 连接光电收发器与交换机的双绞线跳线应当为直通线。有些光纤收发器提供一个

MDI/MDI-X 开关按钮，当使用交叉线时应当按下 MDI/MDI-X 开关按钮，而使用直通线时，则无需按下该按钮。事实上，只要 LED 指示灯变绿即为连通状态，否则，说明连接跳线或开关按钮有问题。

- 连接光电收发器与光纤配线架的光纤跳线通常为 ST-SC，SC 端连接至光电收发器，ST 端连接至光纤配线架。
- 光纤跳线的类型与芯径必须与布线中使用的光纤完全相同。
- 由于光纤端口不具有自适应功能，因此光电收发器与交换机的光纤端口必须采用相同的传输速率和双工模式。

4.5.2 双绞线端口的连接

无论是 10Base-T 以太网、100Base-TX 快速以太网还是 1000Base-T 千兆位以太网，级联交换机所使用的电缆长度均可达到 100 m，这个长度与交换机到计算机之间的长度完全相同。因此，级联除了能够扩充端口数量外，另外一个用途就是快速延伸网络直径。当有 4 台交换机级联时，网络跨度就可以达到 500 m。这样的距离对于位于同一座建筑物内的小型网络而言已经足够了！

■ 使用智能端口级联

最新款的交换机（包括 Cisco 交换机在内）基本上都支持智能翻转端口。所谓智能翻转端口，就是交换机中的所有 RJ-45 端口都能够智能判断对端所连接的是普通网络终端，还是其他网络设备，并自动将端口的类型切换到与之相适应的类型（MDI-II 或 MDI-X），从而实现与对端设备的正常连接。因此，只需使用直通线即可实现网络设备之间的相互连接。

> **提示** 智能翻转端口通常不会在交换机面板上进行标记，因此，必须查看产品的使用手册才能知晓。

■ 使用非智能翻转端口级联

如果相互级联的交换机端口均为非智能翻转端口，那么将只能使用交叉跳线，将两台交换机的普通端口连接在一起，可以扩展网络端口数量（如图 4-60 所示）。

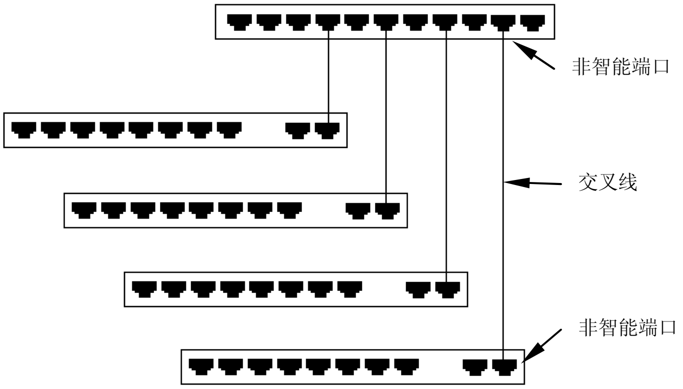


图 4-60　利用交叉线通过非智能翻转端口级联交换机

> **提·示** 当使用非智能翻转端口连接交换机时，必须使用交叉线而不是直通线。

4.6　交换机的堆叠

提供堆叠端口的交换机之间可以通过专用的堆叠线连接起来。通常，堆叠的带宽是交换机端口速率的几十倍。例如，一台 100 Mbps 交换机，堆叠后两台交换机之间的带宽可以达到几百兆位甚至上千兆位。多台交换机的堆叠是靠一个提供背板总线带宽的多口堆叠母模块与单口的堆叠子模块相连实现的，并插入不同的交换机实现交换机的堆叠。

4.6.1 堆叠概述

级联（Uplink）和堆叠（Stack）是多台交换机相互连接在一起的两种方式，主要目的是增加端口密度。级联，是使用跳线将一台交换机的端口与另一台交换机的端口连接在一起。堆叠，是借助专门的堆叠模块，通过交换机的背板连接起来。堆叠是一种建立在芯片级上的连接，将 3 台 48 口交换机堆叠在一起，效果就像是一个 144 口的交换机。

1. 堆叠与级联的区别

堆叠与级联的区别如下。

- 对设备要求不同。级联可通过一根双绞线在任何网络设备厂家的交换机之间，或者交换机与集线器之间完成。而堆叠只有在自己厂家的设备之间，并且该交换机必须具有堆叠功能才可实现。
- 对连接介质要求不同。级联时只需一根跳线，而堆叠则需要专用的堆叠模块和堆叠线缆。当然，堆叠模块是需要另行订购的。
- 最大连接数量不同。交换机间的级联，在理论上没有级联级数的限制。但是，叠堆内可以容纳的交换机数量，各厂商都会明确地进行限制。
- 管理方式不同。堆叠后的数台交换机在逻辑上是一个被网管的设备，可以对所有交换机进行统一的配置与管理。而相互级联的交换机在逻辑上是各自独立的，必须依次对其进行配置和管理每台交换机。
- 设备间连接带宽不同。多台交换机级联时会产生级联瓶颈，并将导致较大的转发延迟。例如，4 台百兆位交换机通过跳线级联时，彼此之间的连接带宽也是 100 Mbps。当连接至不同交换机上的计算机之间通信时，也只能通过这条百兆位连接，从而成为传输的瓶颈。同时，随着转发次数的增加，网络延迟也将变得很大。而 4 台交换机通过堆叠连接在一起时，堆叠线缆将能提供高于 1 Gbps 的背板带宽，从而可以实现所有交换机之间的高速连接。尽管级联时交换机之间可以借助链路汇聚技术来增加带宽，但是，这是以牺牲可用端口为代价的。
- 网络覆盖范围不同。交换机可以通过级联成倍地扩展网络覆盖范围。例如，以双绞线

网络为例，一台交换机所覆盖的网络直径为 100 m，2 台交换机级联所覆盖的网络直径就是 300 m，而 3 台交换机级联时的直径就可达 400 m。而堆叠线缆通常只有 0.5～1 m，仅仅能够满足交换机之间互连的需要，不会对网络覆盖范围产生影响。

2. 堆叠的优点

堆叠是交换机扩展端口的重要方式。堆叠的优点主要包括以下几个方面。

■ **高密度端口**

不同品牌的交换机支持堆叠的层数有所不同，一般情况下，最少可堆叠 2 层，而最多可堆叠至 8 层，因此可在一个狭小的空间内为密集的计算机网络提供上百个端口。

■ **高速传输**

由于叠堆中所有的计算机都连接至同一高速背板模块，位于不同交换机端口的计算机之间的通信不再需要层层转发，减少了交换机之间的转发延迟，避免了端口冲突，所有端口的计算机间均可以线速进行交换，提高了不同交换机间计算机的通信速率。

■ **便于管理**

一个堆叠的若干台交换机可视为一台交换机进行管理，只需赋予其 1 个 IP 地址，即可通过该 IP 地址对所有的交换机进行管理，从而大大减少了管理的强度和难度，极大地节约了管理成本。

需要注意的是，并不是所有的交换机都支持堆叠的，这取决于交换机的品牌，甚至是型号是否支持堆叠。

4.6.2 StackWise 堆叠技术

1. StackWise 堆叠技术简介

Cisco Catalyst 3750/3750G 均支持 StackWise 堆叠技术，可以将多至 9 台的 Cisco Catalyst 3750 交换机堆叠在一起（如图 4-61 所示），创建一个 32 Gbps 的逻辑堆叠交换架构，提供高达 468 个 10/100 Mbps 端口或 252 个 10/100/1000 Mbps 端口。同一堆叠中的所有交换机共享配置和路由信息，从而创建一个单一的交换单元，就好像是一整台交换机一样。

图 4-62 所示为 Cisco Catalyst 3750 交换机的 StackWise 堆叠端口。

只需简单地使用 StackWise 堆叠电缆，将不同的堆叠端口连接在一起，即可实现 Cisco Catalyst 3750 交换机之间的 StackWise 堆叠，如图 4-63 所示。

图 4-61 StackWise 堆叠技术

图 4-62　StackWise 堆叠端口

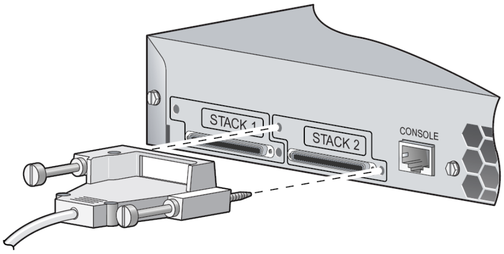


图 4-63　StackWise 堆叠电缆连接

2.　StackWise 堆叠技术特点

StackWise 堆叠技术具有以下特点。

- 构造简单

无需专用管理交换机，堆叠中的每台交换机都能够充当管理层次中的主交换机或从交换机，由从堆叠成员交换机中选出的一台主交换机负责管理。一个堆叠中最多可连接 9 台交换机，并将它们整合为一个统一的、逻辑的、针对融合而优化的设备，从而让客户可以更加放心地部署语音、视频和数据应用。

- 易于管理

每个 StackWise 堆叠都拥有一个单一的 IP 地址，并且作为一个统一的对象进行管理。单一 IP 管理适用于包括故障检测、虚拟 LAN（VLAN）创建和更改、安全和 QoS 控制等多种活动。每个堆叠只有一个配置文件，它将被分发给堆叠中的各个成员。这让堆叠中的每台交换机都可以公用相同的网络拓扑、介质访问控制（MAC）地址和路由信息。

- 堆叠互连

利用特殊的堆叠互连电缆和堆叠软件，Cisco StackWise 技术最多可以将 9 台单独的 Cisco Catalyst 3750 交换机连接到一个统一的逻辑单元中。堆叠相当于一个单一的交换单元，由一个从成员交换机中选出的主交换机管理。主交换机可以自动地创建和升级所有的交换信息和可选的路由表。一个工作中的堆叠可以在不中断服务的情况下，添加新的成员或者移除旧的成员。

- 双向流与负载均衡

为了有效地平衡流量负载，分组被分配到两条逻辑计数循环路径上。每条计数循环路径都支持 16 Gbps 的流量，总共支持 32 Gbps。输出队列会计算路径的使用率，以确保流量负载的平衡分配。系统为流量提供服务的方式取决于它的服务等级（CoS）或者差分服务代码点（DSCP）值。低延时的流量会获得较高的优先级。

- 连接冗余

通过特殊的堆叠互连电缆，可将堆叠中的所有交换机组织成一个单一的逻辑单元，从而创建一条双向的封闭环路。如果检测到电缆中存在断点，流量将会立即转到另外一条 16 Gbps 路径上继续转发。次秒级定时机制可以检测流量故障，及时地进行故障切换，并在检测到电缆上的互动时重新恢复双路径传输。需要注意的是，任何一条电缆发生中断，都将导致堆叠的带宽降低到它的总容量的一半。

- 热插拔

用户可以在不影响堆叠性能的情况下，在一个工作中的堆叠中添加或者移除交换机。堆

叠将会搜集包括交换表在内的各种信息，并在获得新地址之后更新 MAC 地址。网络管理员不需要对交换机进行任何配置，就可以直接使用该交换机。同样，用户也可以在不对剩余交换机产生影响的情况下，从一个工作中的堆叠中移除交换机。当堆叠发现一系列端口不再可用时，它将在不影响转发或者路由的情况下更新相关信息。

3. StackWise 堆叠方式

StackWise 堆叠方式有两种，即全带宽的冗余连接方式（如图 4-64 所示），以及半带宽的非冗余连接方式（如图 4-65 所示）。为了保证连接的安全和获得更高的带宽，建议采用全带宽的冗余连接方式。

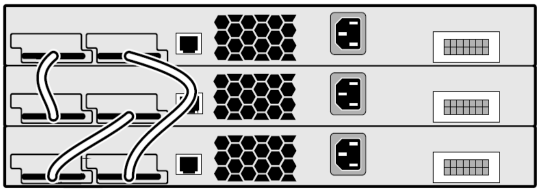


图 4-64　全带宽的冗余连接方式

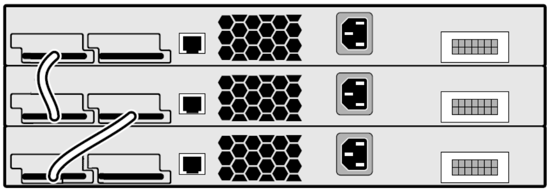


图 4-65　半带宽的非冗余连接方式

图 4-66 所示为采用 0.5 m StackWise 电缆，实现 9 台交换机全带宽冗余连接的方式。

图 4-67 所示为采用 0.5 m 和 3 m StackWise 电缆，实现 9 台交换机全带宽冗余连接的方式。

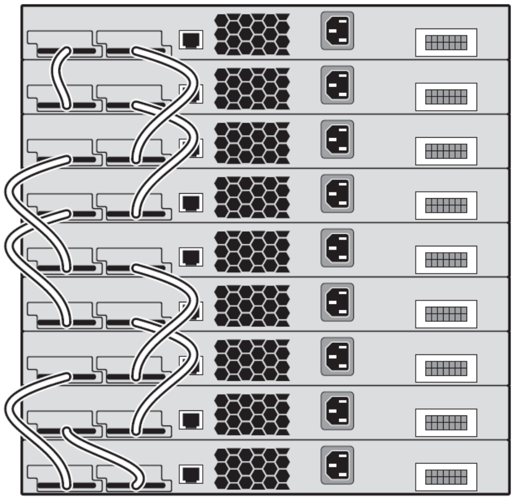


图 4-66　StackWise 冗余连接（1）

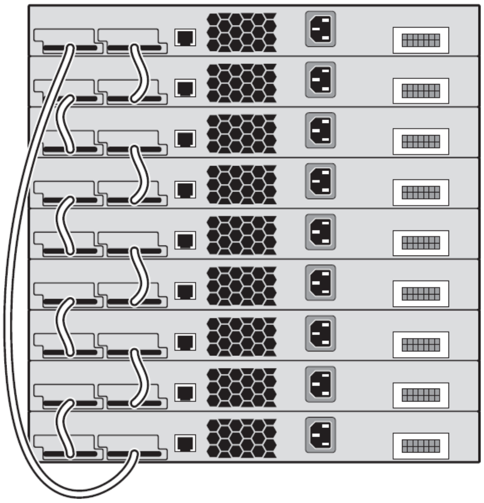


图 4-67　StackWise 冗余连接（2）

图 4-68 所示为采用 0.5 m 和 3 m StackWise 电缆，实现 9 台交换机全带宽冗余连接的另外一种方式。

交换机连接完成之后，也应当借助理线器和尼龙扎带对跳线作必要的整理。同时，建议使用不同颜色的跳线，并在跳线两端应当分别做好标记，以便于在管理时能够弄清该跳线所连接的两端端口。

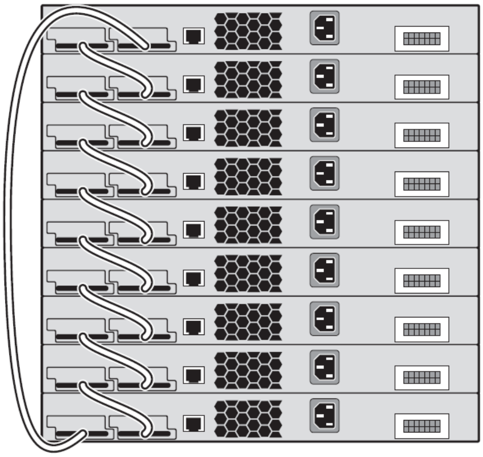


图 4-68　StackWise 冗余连接（3）

4.6.3 StackWise Plus 堆叠技术

StackWise Plus 技术是在获得了极大成功的 StackWise 技术的基础上构建的，后者是一种针对千兆位以太网设计的出色堆叠架构，应用于 Cisco Catalyst 3750-X、Catalyst 3560-X 和 Catalyst 3650 系列交换机。

StackWise Plus 适用于设备的添加、卸载和重新部署，并能保持稳定的性能。堆叠就像是一台交换设备，由从其成员交换机中挑选出的一台主交换机进行管理。主交换机能够自动创建和更新所有交换列表和可选的路由列表。处于工作状态的堆叠能接纳新的成员或卸载旧设备，不会中断服务。StackWise Plus 创建了一个由多达 9 台交换机构成的高度稳定统一系统，利用单一 IP 地址、单一 Telnet 进程、单一命令行接口（Command Line Interface，CLI）、自动版本检查、自动配置等特性简化了管理。

StackWise Plus 不仅支持 StackWise 的所有特性，能够向后兼容现有 Catalyst 3750 系列交换机，而且还将系统吞吐率提高至 64 Gbps。StackWise Plus 还能支持 Catalyst 3750E/3750-X 系列交换机的本地交换功能。从 Catalyst 3750E/3750-X 系列交换机某个端口进入并将从该交换机另一端口输出的本地交换数据包，不必再经过堆叠环，从而进一步提高了交换机的转发性能。

StackWise Plus 的堆叠方式与 StackWise 完全相同，故不复赘述。图 4-69 所示为采用 StackWise Plus 技术堆叠的 Catalyst 3750-X 系列交换机。

图 4-69　StackWise Plus 堆叠

Catalyst 3750-X 系列交换机除数据线可直接堆叠以外，还可以借助专门的电源堆叠电缆（StackPower）实现电源模块的冗余。图 4-70 所示为 XPS-2200 堆叠电源电缆。

图 4-71 所示为使用 StackPower 电缆实现 StackPower 电源堆叠的连接方式。

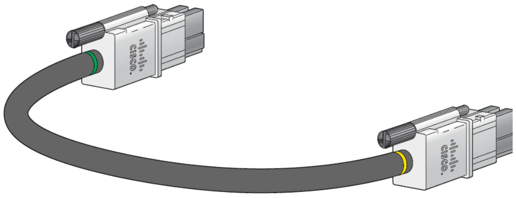


图 4-70　XPS-2200 堆叠电源电缆

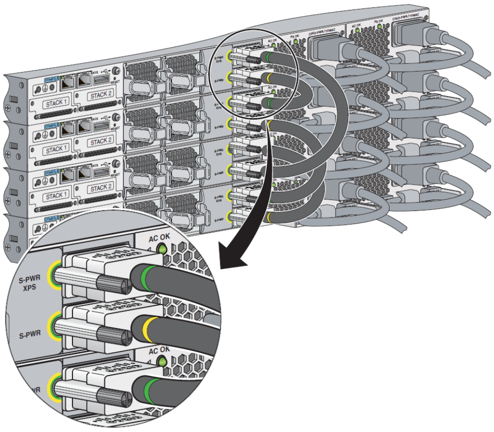


图 4-71　StackPower 电源堆叠

一个 StackPower 堆叠中最多只允许 4 台交换机，而一个 StackWise Plus 则最多允许 9 台交换机。因此，当将 9 台 Catalyst 3750-X 进行堆叠时，需要将其拆分为 3 个 StackPower 堆叠。图 4-72 所示为 StackWise Plus 数据堆叠和 StackPower 电源堆叠的连接方式。

Cisco XPS-2200 作为一个可扩展电源系统，最多可以支持 9 台交换机，并且能够同时为 1～2 台断电的交换机提供电源。当选择使用 XPS-2200 堆叠电源时，StackPower 堆叠的连接方式如图 4-73 所示。

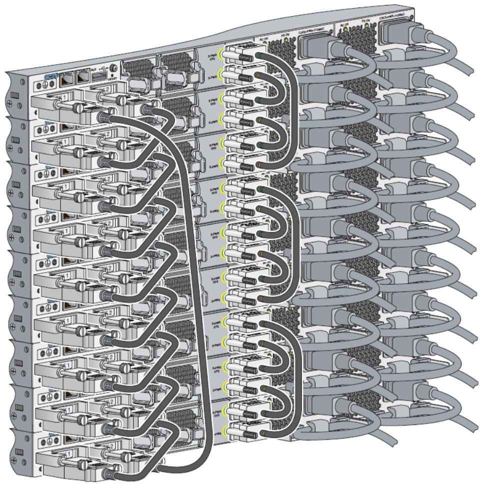


图 4-72　数据和电源堆叠

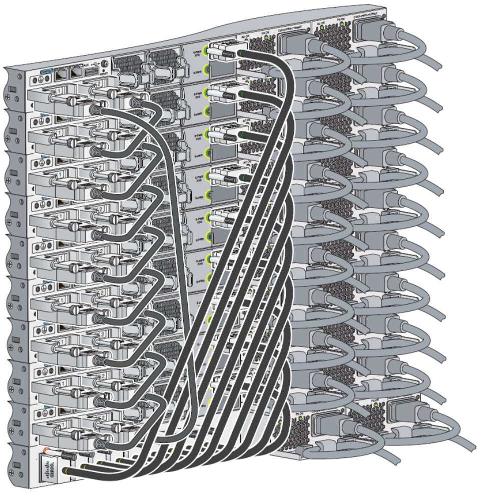


图 4-73　XPS-2200 电源堆叠

4.6.4 FlexStack 堆叠技术

FlexStack 是 Catalyst 2960S 专用的堆叠技术，只适用于 Catalyst 2960S 交换机之间的堆叠。

与 Catalyst 3750 直接提供堆叠模块不同，用于实现 Catalyst 2960S 堆叠的 FlexStack 堆叠模块和线缆必须另行选购。

1. FlexStack 堆叠技术简介

FlexStack 堆叠技术具有以下特点。

- 单点管理。堆叠中的所有交换机都被作为一台逻辑交换机进行配置和管理。每个 FlexStack 堆叠中最多允许 4 台交换机。
- 20 Gbps 连接带宽。两个堆叠成员之间的一个 FlexStack 连接就是一个全双工的 10 Gbps 连接。每个 Catalyst 2960S 成员支持 2 个 FlexStack 连接。每个 FlexStack 成员可以同时使用 2 条堆叠连接以线速发送和接收以太网通信，从而有效地为每个堆叠成员提供 20 Gbps 堆叠带宽。
- 内建冗余和高可用性。高速 FlexStack 连接为每个堆叠成员和其他任何成员之间提供了冗余通信。同时，还将增加与汇聚层交换机之间的冗余连接（如图 4-74 所示）。

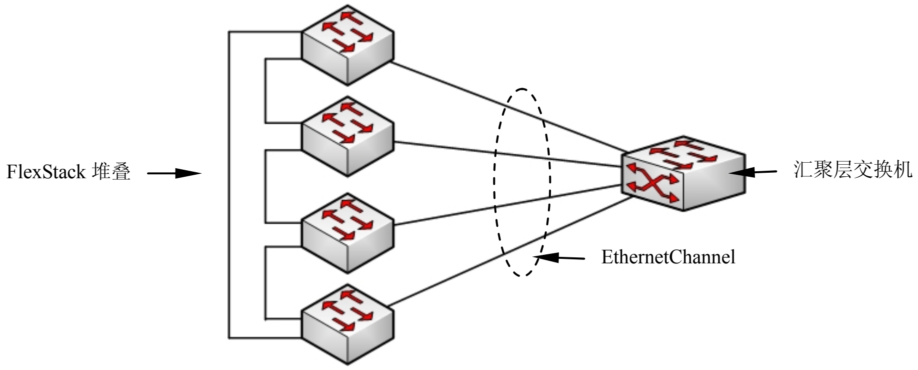


图 4-74　FlexStack 堆叠与汇聚层交换机的连接

- 可伸缩网络需求。向堆叠中安装新的交换机非常简单。当需要增加新的访问接口时，可以随时将新的交换机添加到已经存在的堆叠中。

图 4-75 所示为采用 FlexStack 技术堆叠的 Catalyst 2960S 交换机。

图 4-75　采用 FlexStack 技术堆叠

2. FlexStack 堆叠方式

FlexStack 堆叠电缆分为 0.5 m、1 m 和 3 m 共 3 种规格，可以根据需要选用。若欲采用

FlexStack 方式堆叠 Catalyst 2960S 交换机，应当先为交换机安装 FlexStack 堆叠模块（如图 4-76 所示），然后，再使用 FlexStack 电缆将交换机堆叠在一起。

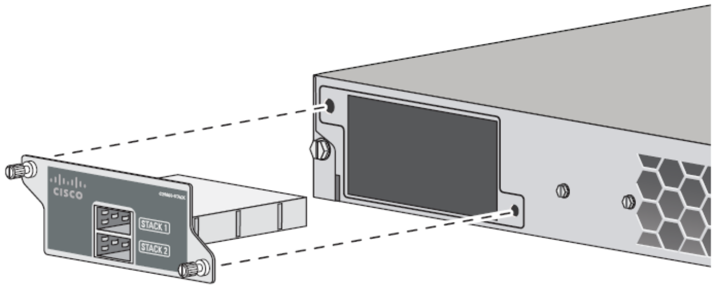


图 4-76　安装 FlexStack 堆叠模块

2 台 Catalyst 2960S 交换机堆叠时，采用 0.5 m FlexStack 线缆，采用如图 4-77 所示方式连接。

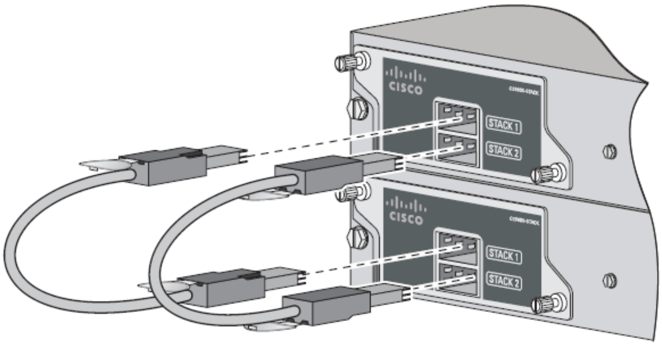


图 4-77　2 台 Catalyst 2960S 交换机堆叠

3 台 Catalyst 2960S 交换机堆叠时，可以全部采用 0.5 m FlexStack 线缆。堆叠的连接方式如图 4-78 所示。

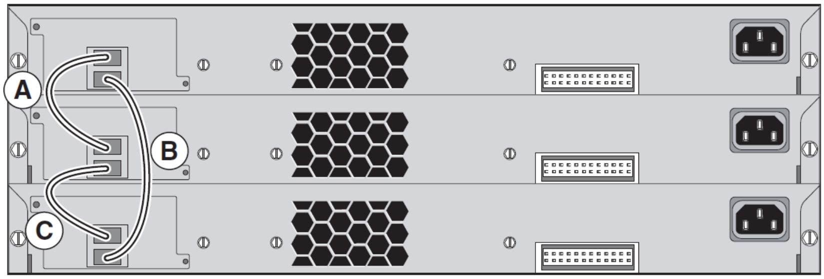


图 4-78　3 台 Catalyst 2960S 交换机堆叠

4 台 Catalyst 2960S 交换机堆叠时，也可以全部采用 0.5 m FlexStack 线缆。堆叠的连接方式如图 4-79 所示。

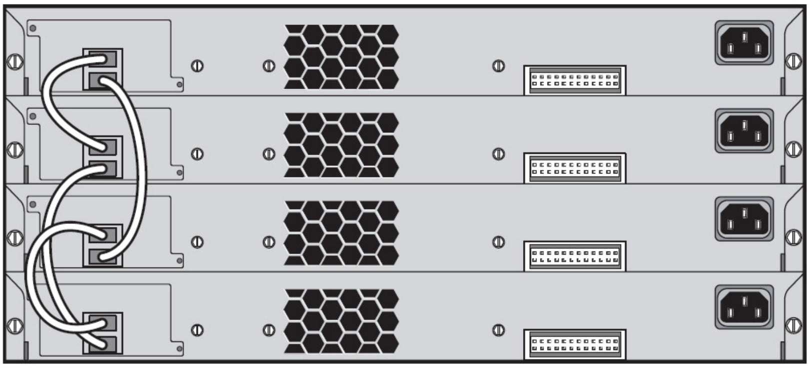


图 4-79　4 台 Catalyst 2960S 交换机堆叠（方式 1）

4 台 Catalyst 2960S 交换机堆叠时，还可以采用 3 条 0.5 m FlexStack 线缆和 1 条 3 m FlexStack 线缆。堆叠的连接方式如图 4-80 所示。

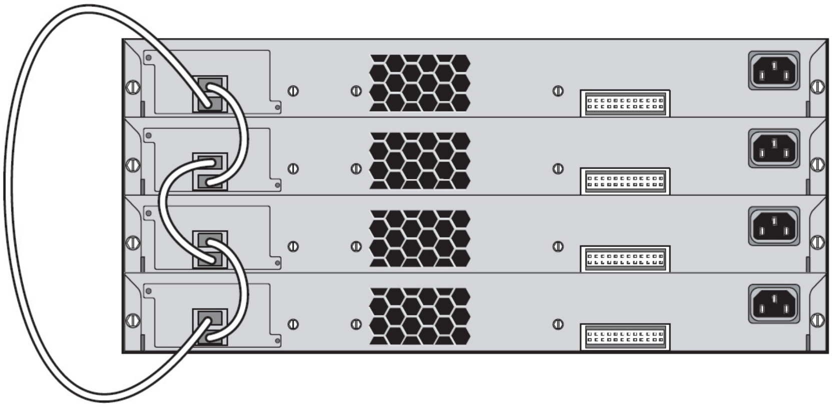


图 4-80　4 台 Catalyst 2960S 交换机堆叠（方式 2）

只有每台 Catalyst 2960S 交换机都拥有 2 条 FlexStack 线缆与其他 Catalyst 2960S 交换机连接时，才能实现连接冗余并提高可用性。如果与其他 Catalyst 2960S 交换机只有 1 条连接，虽然也只能实现基本的 FlexStack 堆叠，但是，当某条 FlexStack 链路中断时，将失去与其他 FlexStack 堆叠成员的联络。

第 5 章　交换机的配置方式与初始化

对于傻瓜交换机而言，所有的管理就是对连接电缆的管理，即连接或终止每个端口所连接的设备。而对于可网管交换机而言，除此之外，还可以通过一些简单的配置，实现网络安全、提高网络通信效率，实现对交换机的远程监控与管理。

5.1　交换机配置前的准备

交换机的配置必须借助于计算机才能实现，也就是说，配置交换机时必须把计算机和交换机连接在一起，使两者之间能够进行正常的通信。

5.1.1　交换机配置前的规划

搭建网络时，通常情况下都是先在网络中心统一配置好交换机，然后再分发到各楼宇的机柜中安装。因此，在动手配置交换机前，必须做好统筹和规划工作，避免可能产生的 IP 地址、名称等各种冲突和混乱。所有规划都必须制作成电子文档，以备配置时参考和日后备查。

1.　IP 地址规划

IP 地址的规划包括以下几个方面的内容。

- 选择网络内使用的 IP 地址范围。如果合法 IP 地址数量较少，建议采用 192.168.0.0～192.168.255.255 或 10.0.0.0～10.255.255.255 段的私有 IP 地址。
- 为每个 VLAN 指定不同的 IP 地址范围，并确定其子网掩码和默认网关，便于为该 VLAN 的计算机分配 IP 地址信息。
- 为每台交换机指定管理使用的 IP 地址信息，便于实现对该交换机的远程管理。交换机管理 IP 地址建议也采用内部保留 IP 地址，如 172.16.0.0～172.16.255.255。

2.　名称规划

名称规划包括以下几个方面的内容。

- 每个端口所连接计算机或用户的名称，用于确认该交换机所连接的计算机或用户，便于日后实现对该端口的远程管理。端口注释中建议包含端口所连接的用户信息、计算机信息或信息模块编号等信息，便于日后对端口的管理。
- 每台交换机的名称，用于确认该交换机所处的位置，便于与其他交换机区分，并对该交换机实现远程管理。交换机名称中建议包含交换机的型号信息、位置信息或用途信息，便于对交换机的识别与管理。
- 每个 VLAN 的名称，用于确认该 VLAN 的性质，便于与其他 VLAN 区分，并实现对

该 VLAN 的管理。VLAN 名称中建议包含部门或分组信息，便于 VLAN 的识别与管理。

3. 安全规划

安全规划包括以下几个方面的内容。

- VLAN 的划分，即将哪些部门或组织单位划分至同一 VLAN，每个 VLAN Trunk 允许哪些 VLAN 通过和访问，以及在哪些交换机上设置哪些 VLAN。
- PVLAN，确定将哪些端口设置为 PVLAN 端口，用于禁止端口之间的相互通信，并借助访问列表实现三层访问控制，从而确保该端口所连接计算机的安全。
- 安全访问列表，确定在哪些交换机上使用哪些访问列表，用于禁止在某个时间段访问网络、禁止访问某些 TCP 或 UDP 端口、禁止使用某些 IP 协议、限制某些 IP 地址范围内计算机的网络访问权限等。
- 安全端口，确定将哪些交换机上的哪些端口设置为安全端口，用于限制连接某个端口的 MAC 地址，以避免非授权计算机访问网络；或者限制某个端口所允许的 MAC 地址数量，以禁止用户私自级联集线设备接入计算机。
- IEEE 802.1x 认证，确定是否采用身份认证的方式实现网络访问安全，以及安全认证服务器如何搭建与配置。
- 传输控制，在哪些端口启用基于端口的传输控制，以保证网络的正常运行，避免可能产生的网络拥塞。

4. 堆叠规划

堆叠规划包括以下几个方面的内容。

- 哪些交换机以堆叠方式实现相互连接，是否拥有必要的堆叠模块。相互通信频繁的大型办公网络可以采用堆叠方式，否则，进行堆叠意义不大。
- 采用何种方式实现堆叠连接。冗余连接方式还是非冗余连接方式，全带宽模式还是半带宽模式。如果条件允许，尽量采用全双工、冗余方式进行堆叠，以提高彼此之间的传输带宽，并提供高可用性。
- 对堆叠如何管理。采用单一 IP 地址管理，还是分别管理。

5. 功能规划

功能规划主要包括以下几个方面的内容。

- EtherChannel，确定是否采用 EtherChannel 来增加网络带宽、提供链接冗余和负载均衡，在哪些网络设备的哪些端口之间的连接上采用 EtherChannel。
- PortFast，确定是否采用 PortFast 减少计算机连接网络的时间，避免长时间的等待。
- QoS，确定是否采用 QoS，以保证视频会议等即时信息的无阻塞传输。
- 多播，确定是否采用多播，以减少网络流量，节约网络带宽。规划并分配多播的 IP 地址。

5.1.2 交换机的管理方式

通常情况下，可以通过两种手段实现配置用于计算机与交换机之间的连接，即通过 Console

端口和 MGMT 端口直接连接的方式，以及通过集线设备间接连接的方式。

1. 外部配置源

由于交换机没有自己的输入和输出设备，因此，在对交换机进行配置时，一般都是通过另一台计算机连接到交换机的配置接口或管理接口上进行配置。对交换机可以采用多种方式进行配置，如图 5-1 所示。

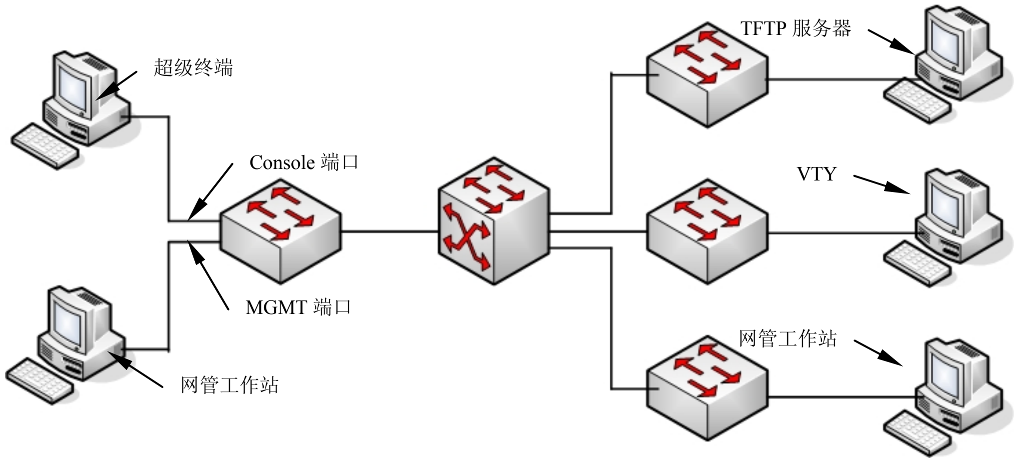


图 5-1 外部配置源

- 控制台

将计算机的串口（COM 口）通过 Console 线与交换机的 Console 端口相连，在计算机上运行终端仿真软件（如超级终端），与交换机进行通信，完成交换机的配置。

- 虚拟终端（Telnet）

如果交换机已有一些基本配置，至少有一个端口有效（如 Ethernet 口），就可通过运行 Telnet 程序的计算机作为交换机的虚拟终端与路由器建立通信，完成交换机的配置。

- 网管工作站

交换机可通过运行网络管理软件的工作站配置，如 Cisco 的 Cisco CNA、CiscoWorks 和 HP 的 OpenView 等。

- TFTP 服务器

TFTP（Trivial File Transfer Protocol）是一个 TCP/IP 简单文件传输协议，可将配置文件从交换机传送到 TFTP 服务器上，也可将配置文件从 TFTP 服务器传送到交换机上。TFTP 不需要用户名和口令，使用非常简单。

2. 通过 RJ-45 Console 端口直接连接

可网管交换机都拥有专门的 Console 端口，用于实现与计算机的直接连接。一些最基本的、事关设备访问安全的配置，都需要借助 Console 端口完成。当交换机和路由器初始化配置完成后，就可以通过网络中的任何计算机进行远程管理了。

■ Console 端口

可进行网络管理的 Cisco 交换机上都有一个 Console 端口，用于对交换机进行配置和管理。通过 Console 端口连接并配置交换机，是配置和管理交换机必须经过的步骤。虽然除此之外还

有其他若干种配置和管理交换机的方式（如 Web 方式、Telnet 方式等），但这些方式必须通过 Console 端口进行基本配置后才能进行。很简单，其他方式往往需要借助于 IP 地址、域名或设备名称才可以实现，而新购买的交换机显然不可能内置有这些参数。所以，通过 Console 端口连接并配置交换机是最常用、最基本也是网络管理员必须掌握的管理和配置方式。有关 Console 端口的详细内容，请参见第 2 章的内容。

Cisco 交换机的 Console 端口一般采用 RJ-45 端口，某些交换机（如 Catalyst 2960S）也有采用 mini-USB 接口（如图 5-2 所示）。

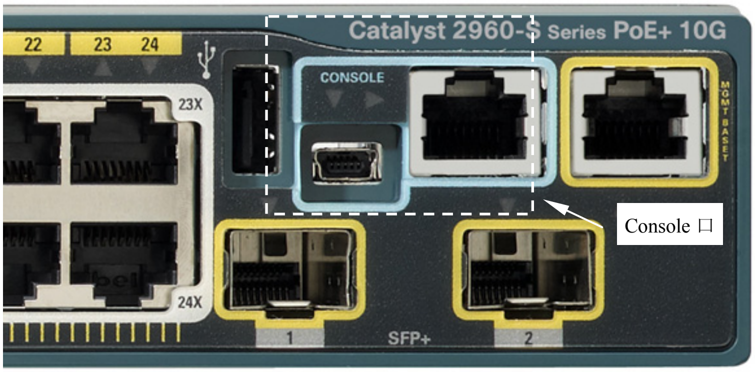


图 5-2　Conlose 端口

■　**Console 线**

配置交换机时，需要通过专门的 Console 线连接至配置用的计算机（通常称作终端）的串行口（COM 口）与交换机的 Console 口。Console 线是一种一端为 DB-9 接头，另一端为 RJ-45 接头的扁平线（RJ-45-to- DB-9），如图 5-3 所示。通常情况下，在交换机的包装箱中都会随机赠送一条 Console 线。

不过，目前几乎所有的笔记本电脑都不再提供 COM 端口，而只提供 USB 接口。因此，或者直接使用台式计算机的 COM 端口配置，或者在笔记本电脑上使用 USB-COM 接口转接器或转接电缆以提供 COM 接口。当然，笔记本电脑的灵活性是台式计算机所无法比拟的，因此，购置一个 USB-COM 接口转接器或转接电缆对于网络管理员而言无疑是一个不错的选择。图 5-4 所示为 USB-COM 转接电缆。另外，还需要为 USB-COM 转换设备安装驱动程序。

图 5-3　Console 线

图 5-4　USB-COM 转接电缆

■ **设备连接**

在利用 Console 线将计算机的串口与交换机的 Console 端口连接在一起之前，应当确认已经做好了以下准备工作。

- 计算机运行正常，并且最好使用便携式计算机（通称为笔记本电脑），这样在移动和操作时都比较方便。
- 计算机中安装有 Windows 9x/Me/2000/XP 操作系统。

> **注·意** Windows Vista 和 Windows 7 操作系统不再提供“超级终端”应用程序，因此，若欲使用该操作系统配置交换机，必须安装其他终端仿真应用程序，如 SecureCRT、WinaXe 等。

- 安装有“超级终端”（Hyper Terminal）组件。如果在附件（Accessories）中没有发现该组件，可通过添加/删除程序（Add/Remove Program）的方式添加该 Windows 组件。
- Console 线缆。
- 为交换机分配的管理 IP 地址、域名或名称。

按照图 5-5 所示的连接方式，利用 Console 线将计算机的串行口（COM 口）与交换机的 Console 端口连接在一起。

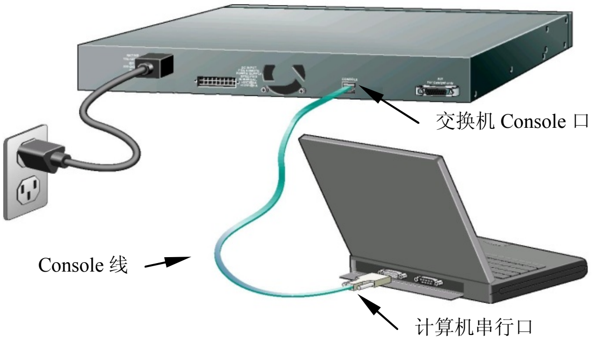


图 5-5　计算机与交换机 Console 端口的连接

> **注·意** Console 线原则上是不允许带电插拔的。至于 USB-COM 转换设备，通常是可以“带电拔插”的。不过，每次拔插时需要先从计算机上拔下 USB 转换器，然后，再将串口设备从转换器上拔下，而不是直接在带电状态下将连接的串口设备拔下（此时对串口来说实际上是单端带电拔插），否则，容易导致设备损坏。

■ **计算机与交换机通信**

在使用超级终端建立与交换机的通信之前，必须先对超级终端进行必要的设置。下面，我们以 Windows XP 为例，简要介绍一下操作过程。

① 利用 Console 线将计算机的串口与网络设备（交换机或路由器）的 Console 端口连接在一起，打开计算机的电源开关。

② 依次选择“开始”→“所有程序”→“附件”→“通信”→“超级终端”命令，显示

如图 5-6 所示的“连接描述”对话框。在“名称”文本框中键入该连接的名称，如 Cisco，用于标识与 Cisco 交换机的连接。

③ 单击“确定”按钮，显示如图 5-7 所示的“连接到”对话框。在连接时使用下拉列表中备选择的串行口，通常为 COM1。

> **注·意** 当采用 USB-COM 转换电缆或转接器时，分配的串行口通常为 COM3/COM4。将转换器插在 USB 口，打开“设备管理器”窗口，选择虚拟出来的串口(不插转换器时是看不到的)，右击鼠标并在快捷菜单中选择“属性”，显示“属性”对话框，在“高级”设置中将端口改成 COM1 或 COM2，这样通用性会好一些。如果终端仿真软件支持 COM3/COM4，也可以不做更改，直接指定所使用的 COM 接口即可。

图 5-6 “连接描述”对话框

图 5-7 “连接到”对话框

④ 单击“确定”按钮，显示如图 5-8 所示的串口属性对话框。在“每秒位数”下拉列表框中选择 9600，其他各选项统统采用默认值。也可直接单击“还原为默认值”按钮，使用应用程序的默认值。

> **注·意** 配置不同厂家的网络设备时，其超级终端的参数设置有所不同，应当认真查看随机提供的技术资料。否则，将无法借助超级终端与网络设备的连接。

⑤ 单击“确定”按钮，显示超级终端窗口。

打开交换机电源后，连续按 Enter 键，即可显示交换机初始界面。图 5-9 所示为 Cisco 4006 交换机初始页面。

计算机与交换机连接成功之后，就可以用菜单（Menus）方式或命令行（Command Line）方式对交换机进行配置和管理了。

> **注·意** 如果在计算机屏幕上未能显示交换机的启动过程，则可能是通信端口选择错误，需重新配置超级终端。当然，也有可能是 Console 线或连接有问题，应当逐一进行检查。

图 5-8 串口属性对话框

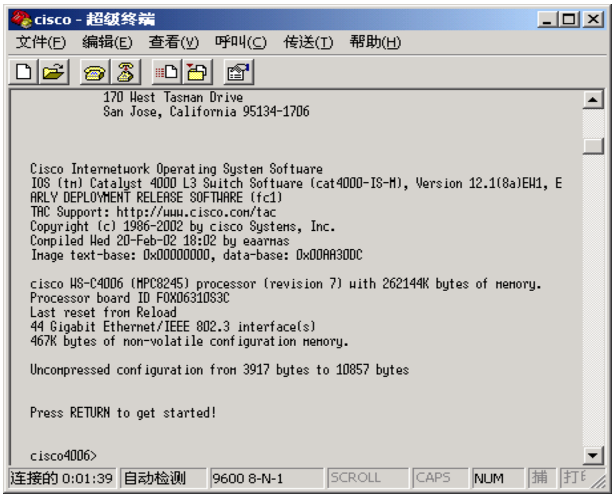


图 5-9 交换机初始页面

3. 通过 mini-USB Console 端口直接连接

Catalyst 2960-S、Catalyst 3560-X、Catalyst 3750-X、Catalyst 3650、Catalyst 3850 等新型交换机都提供了 mini-USB 类型的 Console 端口，可以直接使用 USB 线连接到计算机的 USB 接口进行配置。对于使用笔记本电脑的用户而言，这无疑是非常简捷而方便的方式。

使用 USB 电缆时，交换机与计算机之间的连接方式如图 5-10 所示。

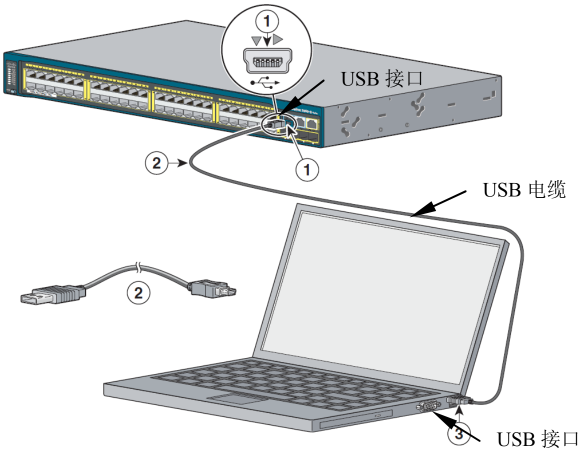


图 5-10 交换机与计算机 USB 端口的连接

不过，在使用 USB 线配置交换机之前，需要先在配置计算机中为交换机安装驱动程序。

① 从 Cisco 官方网站可以下载该驱动（Cisco Virtual Com InstallShield Wizard，文件名为 Cisco_usbconsole_driver.zip。将该文件解压缩后，如果使用 32 位 Windows XP 系统，在“Windows_32”文件夹双击 setup.exe；如果使用 64 位 Windows XP，在“Windows_64”文件夹双击 setup(x64).exe，即可运行“Cisco Virtual Com InstallShield Wizard”（Cisco 虚拟 COM 安装向导）安装向导（如图 5-11 所示）。

② 使用 USB 线缆将交换机的 Console 端口连接至计算机，USB Console 端口的 LED 指示

灯变为绿色。

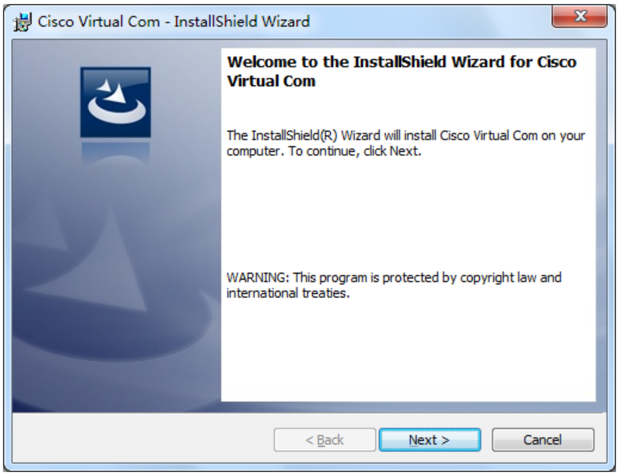


图 5-11 “Cisco Virtual Com InstallShield Wizard”安装向导

③ Windows 将自动运行“发现新硬件向导”，并完成驱动程序的安装。

④ USB Console 已经可以使用。然后，使用终端仿真程序（如超级终端）配置和管理交换机。

4. 通过 MGMT 端口连接

■ MGMT 端口简介

MGMT 或称 MGT（Management Port，管理端口）是一个可以连接计算机的三层主机端口（如图 5-12 所示），只需使用一条双绞线跳线，就可以将计算机的以太网端口与交换机的 MGMT 端口连接在一起，实现对交换机的配置与管理。也就是说，可以使用 MGMT 端口代替 Console 端口实现对交换机或交换机堆叠的网络管理。

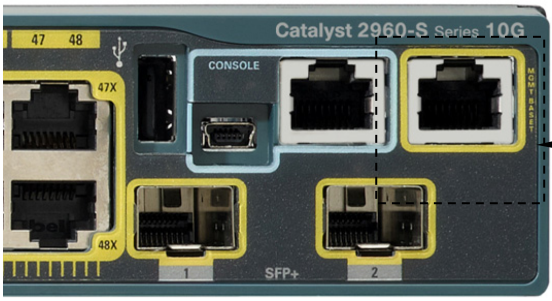


图 5-12 MGMT 端口

> **提·示** MGMT 端口既可用于交换机的初始化，也可以在交换机初始化完成后，以 Telnet、Web 浏览器或 Cisco CNA 方式进行管理。

当将计算机连接到独立的交换机时，连接方式如图 5-13 所示。

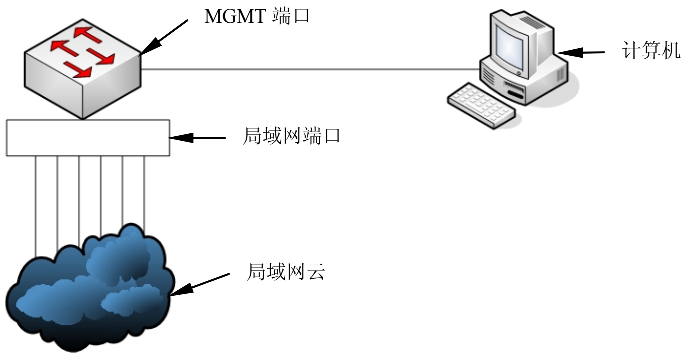


图 5-13　连接 MGMT 端口

当管理交换机堆叠时，也可以将计算机连接到交换机堆叠中任一成员的 MGMT 端口（如图 5-14 所示）。所有成员交换机的 MGMT 端口好像处于一个集线器中，主堆叠交换机将连接至配置计算机。当主堆叠交换机失败并选择出新的主堆叠交换机时，计算机将自动连接至新的主堆叠交换机。

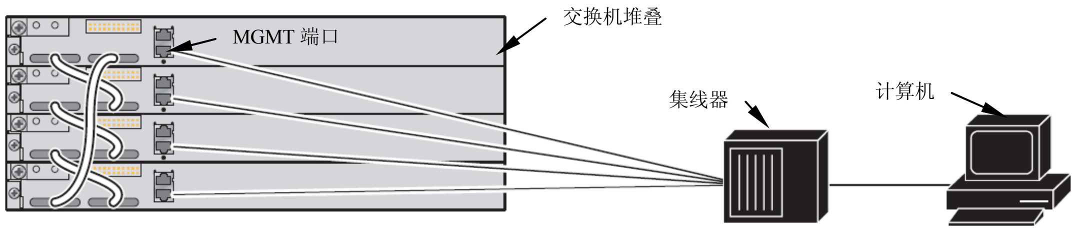


图 5-14　连接交换机堆叠的 MGMT 端口

MGMT 端口支持以下功能和特性。

- 快速设置（只适用于交换机堆叠）
- 网络助理（Network Assistant）
- 带密码的 Telnet
- TFTP
- 安全 Shell（Secure Shell，SSH）
- 基于 DHCP 的认证
- SNMP（只支持 ENTITY-MIB 和 IF-MIB）
- IP Ping
- 接口功能
- 速率（10 Mbps、100 Mbps、1000 Mbps 和自适应）
- 双工模式（全双工、半双工和自适应）
- 环回发现
- CDP（Cisco Discovery Protocol，Cisco 发现协议）
- DHCP 中继代理
- IPv4 和 IPv6 访问列表（Access Control List，ACL）

> **注·意**　在 MGMT 端口上启用某个特性之前，要确认该特性能够被 MGMT 所支持。如果尝试配置不被 MGMT 端口支持的功能，不仅特性配置无法实现，甚至还可能会导致交换机失败。

■ **配置 MGMT 端口**

在 CLI 中，Catalyst 2960S/3560-X/3560E/3750-X/3750E 等系列交换机使用 Fa0 或 fastethernet0 指定 MGMT 端口，Cisco Catalyst 4500 E-Series Supervisor Engine 6L-E 管理引擎使用 fa1 或 fastethernet1 指定 MGMT 端口等。

若欲禁用 MGMT 端口，则需要在接口配置命令中键入 shutdown；若欲启用 MGMT 端口，则需要在接口配置命令中键入 no shutdown。

若欲查看 MGMT 端口与计算机的连接状态，可以查看 MGMT 端口的 LED 指示灯。当连接被激活时，该 LED 指示灯呈绿色；当连接失败时，LED 指示灯将熄灭。

使用 show interfaces fastethernet 0 特权配置命令，可以查看 MGMT 端口与计算机的连接状态。

> **提·示**　计算机的 IP 地址信息设置，应当与被管理交换机位于同一网段。否则，将不能实现彼此之间的通信。可以使用 ping vrf mgmtVrf *ip_address* 命令，测试 MGMT 端口与其他设备的连通性。

5. 通过网络远程连接

计算机除了可以通过交换机的 Console 端口直接连接外，还可以通过交换机的普通端口进行连接。也就是说，只需将网管计算机连接至网络，即可实现对网络中所有可网管交换机的远程监控与管理，如图 5-15 所示。不过，通过普通端口对交换机进行管理时，就不再使用超级终端了，而是以 Telnet 或 Web 浏览器的方式实现与被管理交换机的通信。当然，实现这种连接的前提是必须已经为交换机配置好 IP 地址。否则，计算机根本无法找到欲管理的交换机，并与之进行通信。

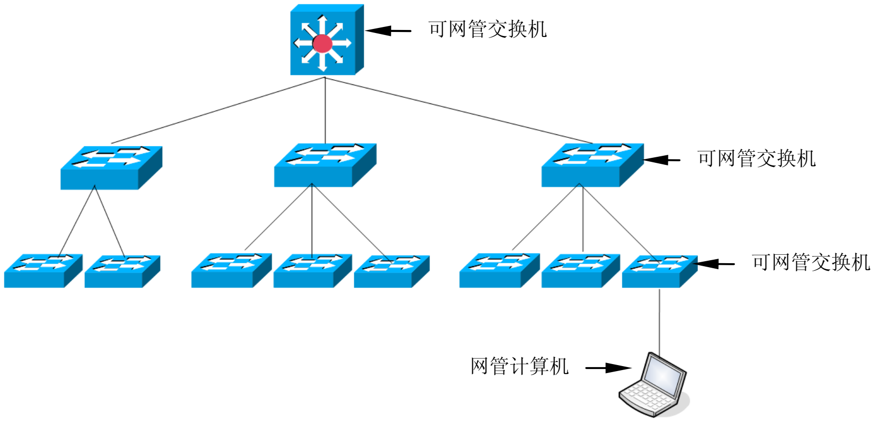


图 5-15　可网管交换的远程管理

5.1.3 交换机的配置方式

1. 超级终端

① 运行超级终端，在图 5-16 所示的“连接到”对话框中的“连接时使用”下拉列表中选择“TCP/IP（Winsock）”选项，然后在“主机地址”文本框中键入欲管理的交换机或路由器的 IP 地址，“端口号”采用默认值 23。

② 单击“确定”按钮，显示如图 5-17 所示的超级终端窗口，实现与被管理设备的连接。

图 5-16 “连接到”对话框

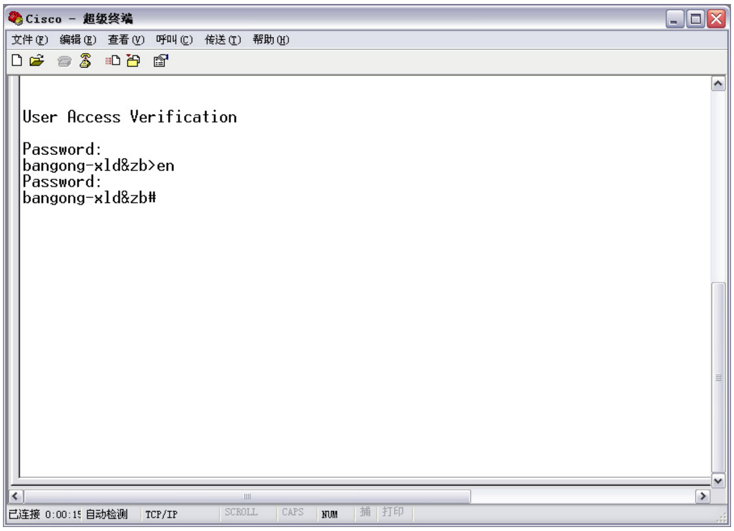


图 5-17 超级终端窗口

2. Telnet

Telnet 协议是一种远程访问协议，可以用它登录到远程计算机、网络设备或专用 TCP/IP 网络。Windows XP/7/8 内置有 Telnet 客户端程序，用于实现与远程交换机的通信。

> **注·意** Windows 7/8 默认不再提供 Telnet 功能。因此，应当执行以下操作：控制面板→程序和功能→打开或关闭 Windows 功能→Telnet 客户端。

在使用 Telnet 连接至交换机前，应当确认已经做好以下准备工作。

- 在用于管理的计算机中安装有 TCP/IP 协议，并配置好了 IP 地址信息。
- 在被管理的交换机上已经配置好 IP 地址信息。如果尚未配置 IP 地址信息，则必须通过 Console 端口进行设置。
- 在被管理的交换机上建立了具有管理权限的用户账户。如果没有建立新的账户，则 Cisco 交换机默认的管理员账户为 Admin。

在计算机上运行 Telnet 客户端程序，并登录至远程交换机，操作如下。

依次选择“开始”→“运行”命令，在弹出的对话框中键入 Telnet 命令。命令格式如下：

```
telnet ip_address
```

其中，*ip_address* 表示被管理交换机的 IP 地址。

例如，交换机的 IP 地址为 172.16.100.12，那么，命令格式如下：

```
telnet 172.16.100.12
```

单击“确定”按钮或按 Enter 键，建立与远程交换机的连接。图 5-18 所示是计算机通过 Telnet 与 Cisco Catalyst 3750 交换机建立连接时的页面。

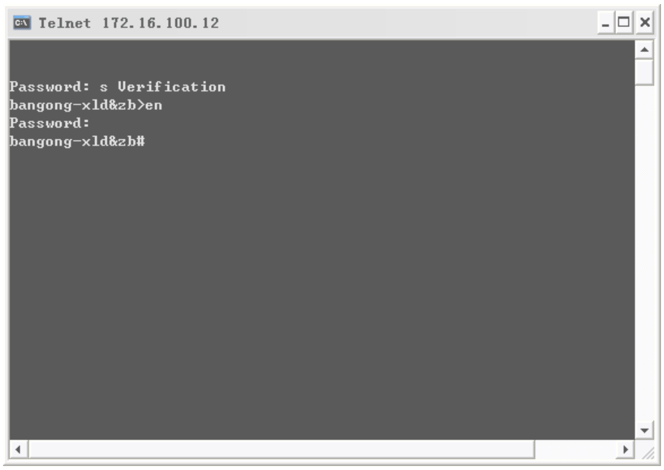


图 5-18　Catalyst 3750 交换机连接界面

然后，就可以根据实际需要对该交换机进行相应的配置和管理了。

> **注·意**　如果通过 MGMT 端口（Fa1）Telnet 远程交换机，使用 telnet <word> /vrf mgmtVrf 命令。其中，word 指远程系统的 IP 地址或主机名。

3. Web 界面

当交换机初始化完成，配置好 IP 地址信息并启用 HTTP 服务后，即可通过支持 Java 的 Web 浏览器访问交换机，并可通过 Web 浏览器修改交换机的各种参数并对交换机进行管理。与 Telnet 冷冰冰的纯字符界面相比，Web 的图形化界面无疑要友好得多，操作起来自然也就更加得心应手。事实上，通过 Web 界面，可以对交换机的许多重要参数进行修改和设置，并可实时查看交换机的运行状态。

在利用 Web 浏览器访问交换机之前，应当确认已经做好以下准备工作。

- 在用于管理的计算机中安装 TCP/IP 协议，并且在用于管理的计算机和被管理的交换机上都已经配置好 IP 地址信息。
- 用于管理的计算机中安装有支持 Java 的 Web 浏览器，如 Internet Explorer 4.0 及其以

上版本、Netscape 4.0 及其以上版本，以及 Oprea with JAVA。

- 在被管理的交换机上建立了拥有管理权限的用户账户和密码。
- 被管理交换机的 Cisco IOS 支持 HTTP 服务，并且已经启用了该服务。否则，应当通过 Console 端口升级 Cisco IOS 或启用 HTTP 服务。

在计算机上运行 Web 浏览器，并连接至被管理交换机。操作如下：

① 运行支持 Java 的 Web 浏览器，在地址栏中键入被管理交换机的 IP 地址（如 172.16.100.100）或为其指定的域名。按 Enter 键，显示如图 5-19 所示的对话框。

图 5-19 用户确认

② 分别在“用户名”和“密码”文本框中键入拥有管理权限的用户名和密码。用户名/密码应当事先通过 Console 端口进行设置。

③ 单击“确定”按钮，建立与被管理交换机的连接，Web 浏览器中显示交换机的管理页面。图 5-20 所示为 Cisco Catalyst 3550 交换机的 Web 管理界面。

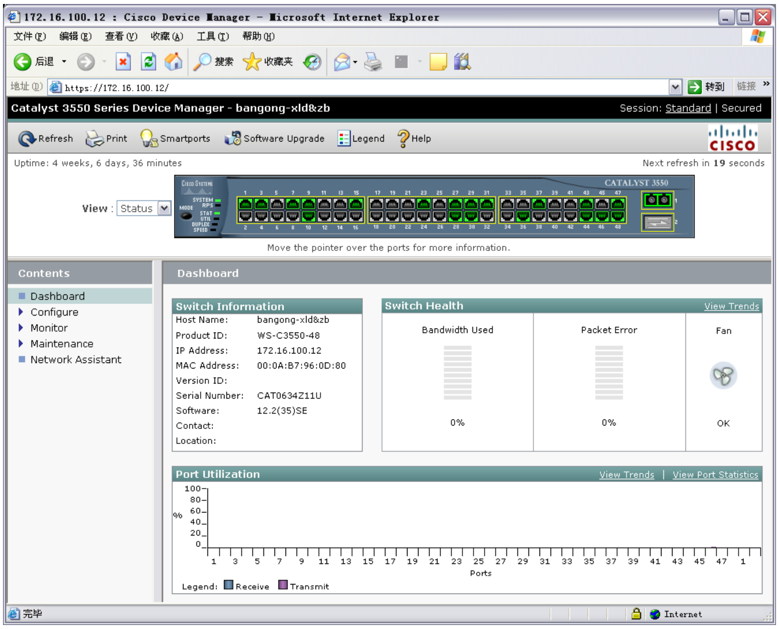


图 5-20 Cisco Catalyst 3550 交换机的 Web 管理界面

接下来就可以通过 Web 界面查看交换机的各种参数和运行状态，并可根据需要对交换机的某些参数做必要的修改。

4. Cisco CNA

Cisco CNA 提供了图形化的配置和管理界面，可以在不使用命令行接口（Command Line Interface，CLI）命令的情况下执行多项配置任务。对于 VLAN 和服务质量设置、设备库存清

单和统计报告、连接和服务监控、软件升级，以及许多其他网络功能，还可以同时对多个设备和端口进行批量管理。

Cisco CNA 是 Cisco 针对来自内部网任何区域的独立设备或设备组（团体和集群）进行管理而开发的实用程序，主要用于管理 Cisco Catalyst 接入系列和汇聚系列交换机，如 Catalyst 4x00 系列、Catalyst 37xx 系列、Catalyst 35xx 系列和 Catalyst 29xx 系列。Cisco CNA 完全免费，可以从 Cisco 官方网站（http://www.cisco.com）下载中文或英文版本安装使用。

> **提·示**　虽然 Cisco CNA 号称也能管理中低端路由器、PIX 或 ASA 防火墙及无线接入设备，但是，最多也只是能够发现这些设备而已，并不能实现真正的管理。若欲管理路由器，可以借助 Cisco SDM；若欲管理防火墙，可以借助 Cisco ASDM；若欲管理无线接入设备，则可以借助 WCS。

Cisco Network Assistant 提供了两种设备组视图模式。

■　**拓扑视图**

拓扑视图（如图 5-21 所示）显示团体、集群中或有资格加入团体或集群的设备、设备之间的链接信息，以及其他所连接的集群。在拓扑图中可以直观地看出哪些设备可以被管理（连接较粗），哪些设备之间是冗余链路（双线），哪些设备出现问题（设备上标记有黄色叹号）。

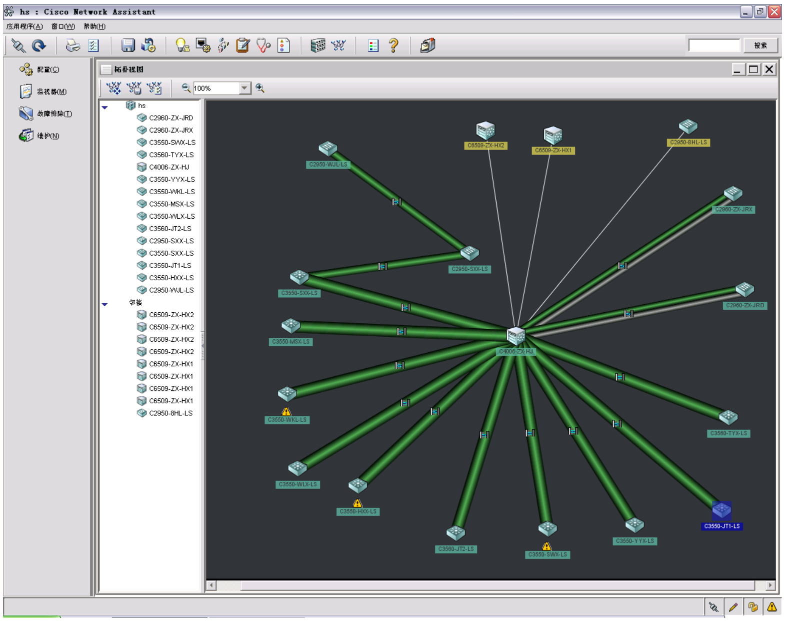


图 5-21　拓扑视图

■　**前面板视图**

从前面板视图（如图 5-22 所示）中可以监控设备的实时状态，并实行多种配置任务。视图中的设备和端口 LED 状态显示与物理设备和端口实际状态基本相同。

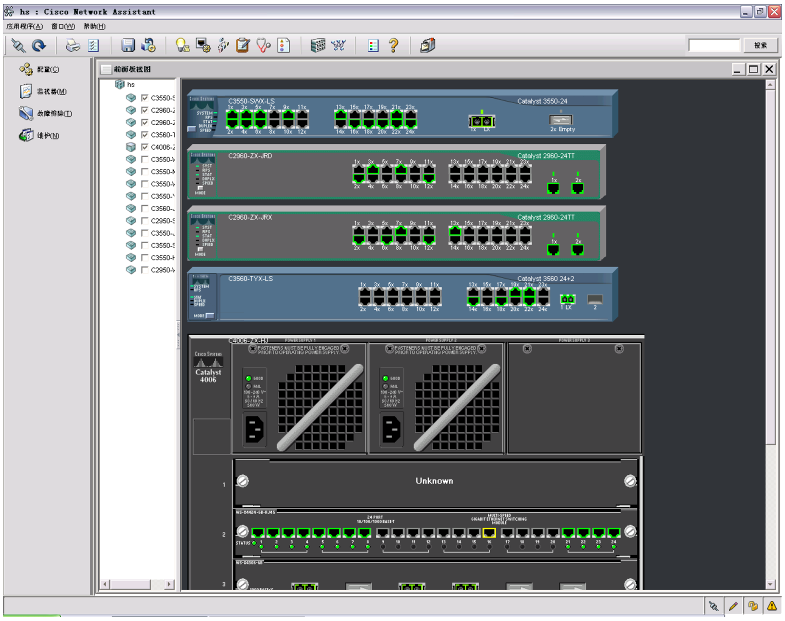


图 5-22　前面板视图

5.1.4　配置信息准备

在配置交换机，特别是多台交换机前，应当先做好以下准备工作。

- 管理 IP 地址信息。包括 IP 地址、子网掩码和默认网关。通常情况下，交换机的管理 IP 地址应当选择使用保留 IP 地址段，并且应当与内部计算机使用的 IP 地址范围不同。
- 主机名称。每台交换机都应当分配一个主机名称，便于彼此之间的区别，避免针对某台交换机所执行的误操作。
- Enable secret 密码或 Enable 密码。进入交换机全局配置模式，设置对交换机配置和管理所需要的密码。密码通常不少于 8 位，并且应当是没有意义的、大小写英文字母与数字的组合。
- 远程 Telnet 密码。使用 Telnet 或超级终端，设置对交换机远程管理所使用的密码。

5.2　CLI 命令行

尽管交换机可以采用 Web 界面和图形界面进行配置，但是，使用 CLI 命令行配置仍然是最简单、最有效、最快捷、最终极的方式，从某种意义上讲，能否熟练掌握 CLI 命令行，是判断网络管理员水平高低的重要标准。

5.2.1　CLI 命令行及使用

Cisco 交换机使用的操作系统为 Cisco IOS（也使用过 Catalyst OS 系统）。CLI（Command Line Interface）是一个基于命令行的软件系统，对大小写不敏感（即不区分大小写）。与其他

操作系统命令行不同，CLI 可以缩写命令与参数，只要它包含的字符足以与其他当前可用的命令和参数区别开来即可。

> **注·意**　本书中所涉及的命令行示例，除明确说明的以外，全部为 Cisco IOS 命令。

1.　CLI 方式的适用

虽然对交换机的配置和管理也可以通过多种方式实现，既可以使用纯字符形式的命令行和菜单（Menu），也可以使用图形界面的 Web 浏览器，甚至专门的网管软件（如 Cisco CNA）。相比较而言，命令行方式的功能更强大，但掌握起来难度也更大一些。

通过 CLI 配置和管理交换机，既可采用 Console 线直接连接至 Console 端口的方式，也可采用通过集线设备间接连接至被管理交换机的方式。不过，当使用后一种方式时，需要事先为交换机配置好 IP 地址信息。然后，采用 Telnet 或超级终端从远程计算机连接至被管理交换机。图 5-23 所示为 Cisco Catalyst 3550 的 CLI 用户界面。

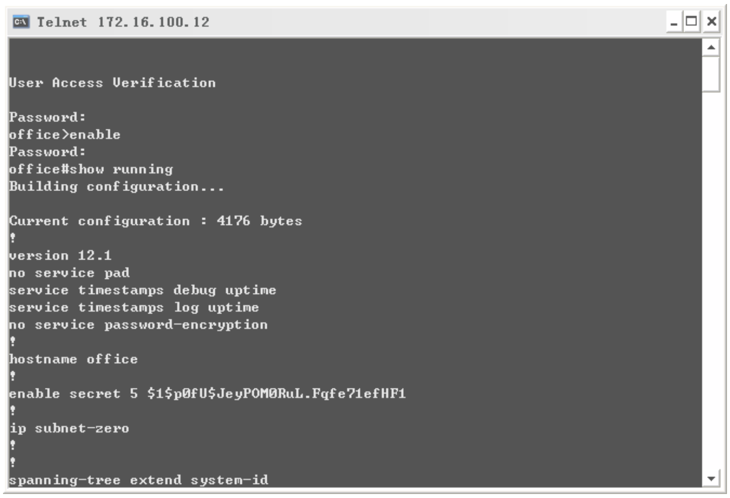


图 5-23　CLI 用户界面

2.　CLI 命令模式

Cisco IOS 命令需要在各自的命令模式下才能执行。因此，如果想执行某个命令，必须先进入相应的配置模式。例如，interface type_number 命令只能在 Global configuration（全局配置）模式下执行，duplex full-flow-control 命令只能在 Interface configuration（接口配置）模式下执行。

Cisco IOS 共包括 7 种不同的命令模式：User Exec（用户）模式、Privileged Exec（特权）模式、Global（全局）配置模式、Config-vlan 模式、VLAN Configuration 模式、Interface（接口）Configuration 模式和 Line Configuration 模式。当在不同的模式下，CLI 界面中会出现不同的提示符。表 5-1 列出了 6 种 CLI 命令模式的用途、提示符、访问及退出方法。

表 5-1 CLI 命令模式摘要

模 式	访问方法	提 示 符	退出方法	用 途
User Exec	开始一个进程	switch>	键入 logout 或 quit	改变终端设置执行基本测试，显示系统信息
Privileged Exec （enable）	在 User Exec 模式中键入 enable 命令	switch#	键入 disable 退出	校验键入的命令。该模式由密码保护
Global Configuration	在 Privileged Exec 模式中键入 configure 命令	switch （config）#	键入 exit 或 end 或按 Ctrl+Z 组合键，返回至 Privileged Exec 状态	将配置的参数应用于整个交换机
VLAN configuration	在 Global Configuration 模式中键入 vlan vlan-id	switch （config-vlan）#	键入 exit 退回至 Global Configuration 模式；按 Ctrl+Z 组合键或键入 end，返回至 Privileged Exec 模式	配置 VLAN 参数。当 VTP 模式处于透明模式时，创建扩展序列的 VLAN（VLAN ID 大于 1005），并将配置文件保存至启动文件
Interface Configuration	在 Global Configuration 模式中，键入 interface 命令	switch （config-if）#	键入 exit 返回至 Global Configuration 模式，按 Ctrl+Z 组合键或键入 end，返回至 Privileged Exec 模式	为 Ethernet interface 配置参数
Line Configuration	在 Global Configuration 模式中，键入 link console 0 命令	switch （config-line）#	键入 exit 返回至 Global Configuration 模式，按 Ctrl+Z 组合键或键入 end，返回至 Privileged Exec 模式	为 terminal line 配置参数

CLI 各种命令模式的进入流程如图 5-24 所示。

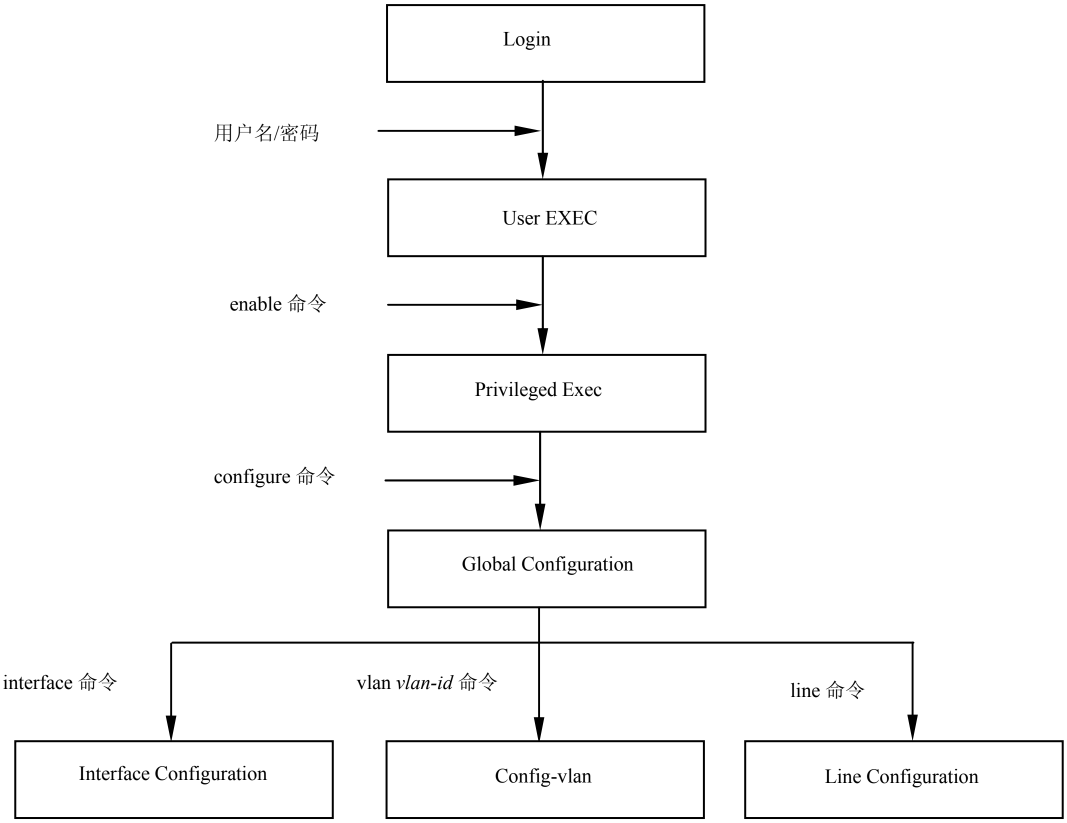


图 5-24 命令模式的进入流程

CLI 各种命令模式的退出流程如图 5-25 所示。

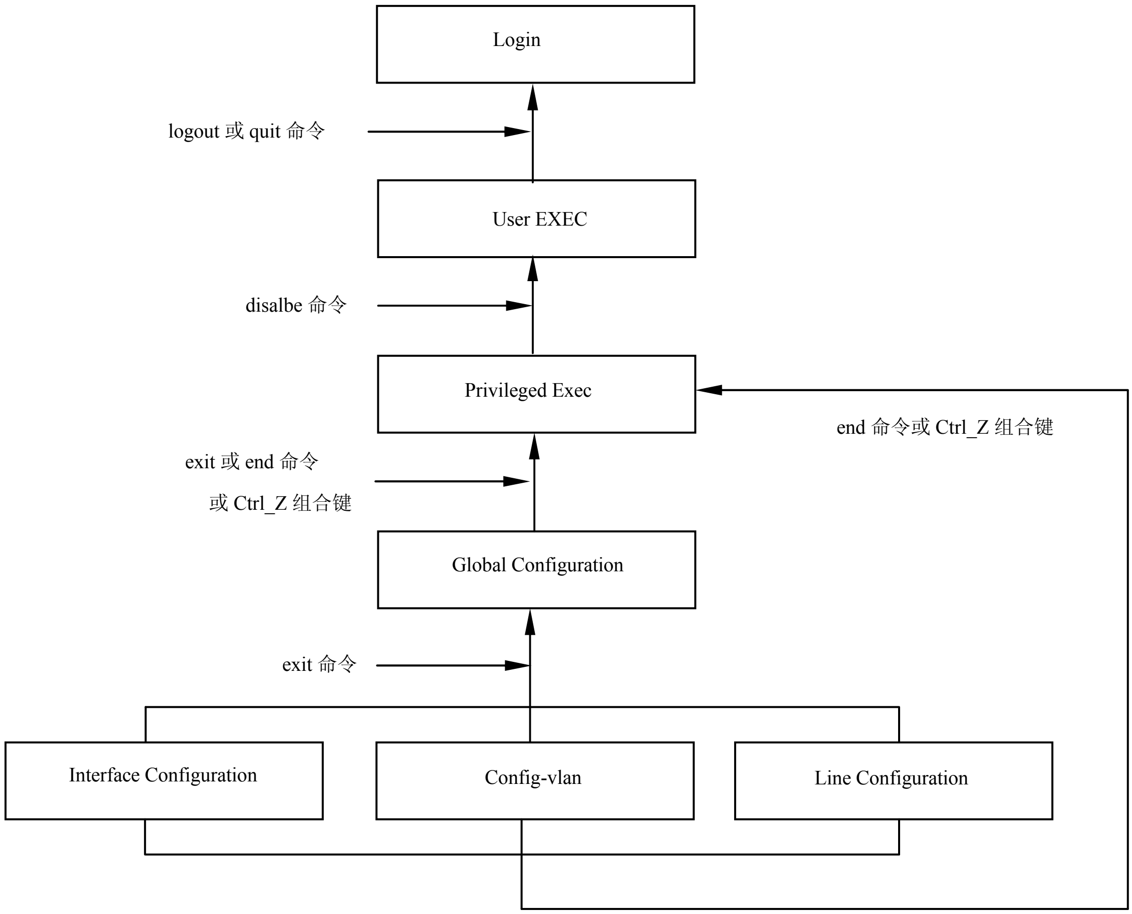


图 5-25　命令模式的退出流程图

命令模式的进入和退出过程如图 5-26 所示。

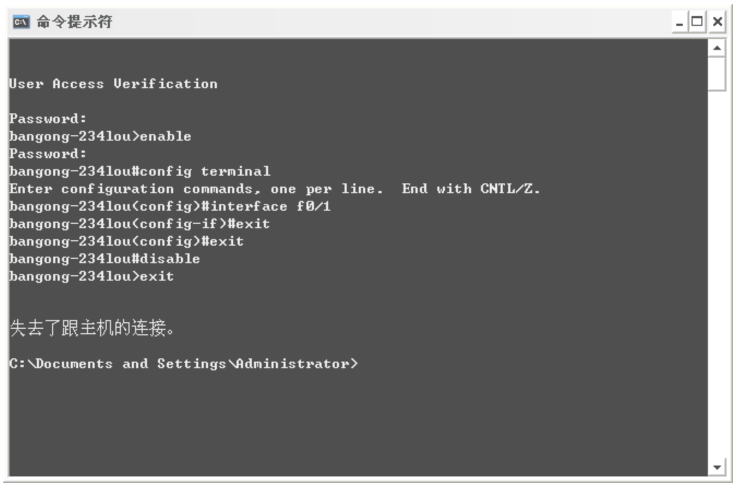


图 5-26　命令模式的进入和退出过程

3. 使用帮助

在任何命令模式下，只需键入？，即可显示该命令模式下所有可用到的命令及其用途。另外，还可以在一个命令和参数后面加？，以寻求相关的帮助。

例如，想看一下在特权配置（Privileged Exec）模式下有哪些命令可用，那么可以在#提示符下键入？，并按 Enter 键，如图 5-27 所示。

图 5-27　键入？查看可用命令

再如，如果想继续查看 Show 命令的用法，那么只需键入 show ?并按 Enter 键即可，如图 5-28 所示。

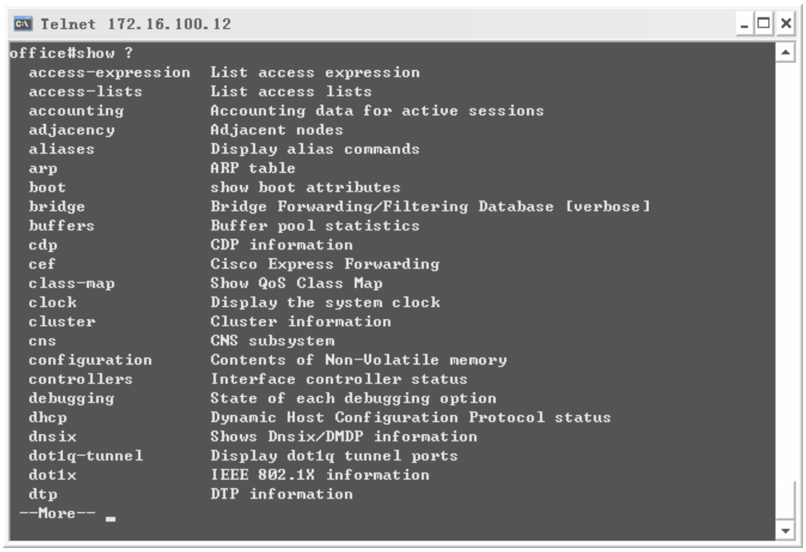


图 5-28　键入 show ？查看用法

另外，?还具有局部关键字查找功能。也就是说，如果只记得某个命令的前几个字符，那么，可以使用？让系统列出所有以该字符或字符串开头的命令。但是，在最后一个字符和？之间不得有空格。例如，在特权配置模式下键入 show c？，系统将显示以 c 开头的所有命令，如图 5-29 所示。

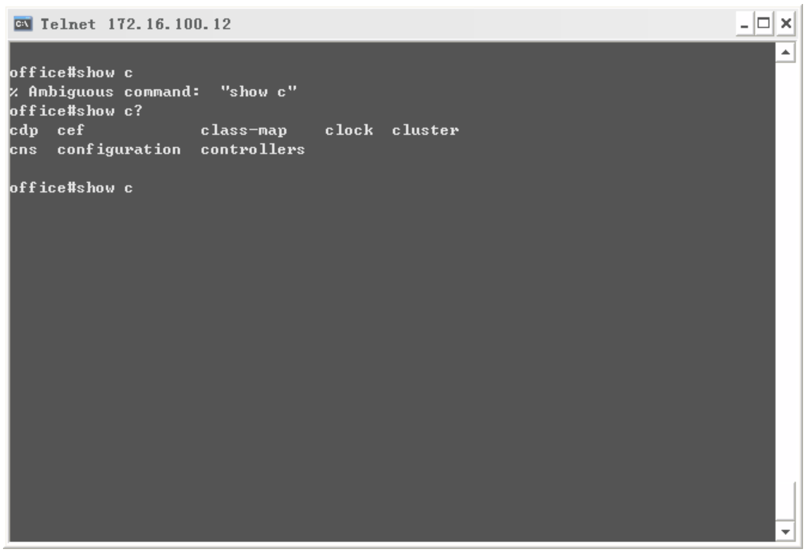


图 5-29 键入 show c？显示以 c 开头的所有命令

此外，在接口配置模式下，使用“?”还可以用来查看可以配置的接口和子接口。如：

```
Router(config)# interface GigabitEthernet ?
<0-0> GigabitEthernet interface number
<0-2> GigabitEthernet interface number
Router(config)# interface GigabitEthernet 1/?
<0-4> Port Adapter number
Router (config)# interface GigabitEthernet 1/3/?
<0-15> GigabitEthernet interface number
Router (config)# interface GigabitEthernet 1/3/8?
. <0-3>
Router (config)# interface GigabitEthernet 1/3/8.0
Router(config-if)#
```

4. 命令的简略方式

在配置过程中，不必键入完整的命令，只要键入的字符足以与其他命令相区别即可。使用缩写命令，无疑将加快命令的键入速度。例如，当欲键入 **show running-config** 命令时，只需键入 **sh run** 即可；当欲键入 **enable** 命令时，只需键入 **en** 即可；当欲键入 **config termanil** 命令时，只需键入 **conf t** 即可。例：想键入 **interface serial 0/0** 命令，只需键入 **int s0/0** 即可，如图 5-30 所示。

另外，若欲重新显示并使用以前曾经键入的命令，可直接使用↑光标键向前翻，即可一一显示已经执行过的命令，按 Enter 键即可重新执行。

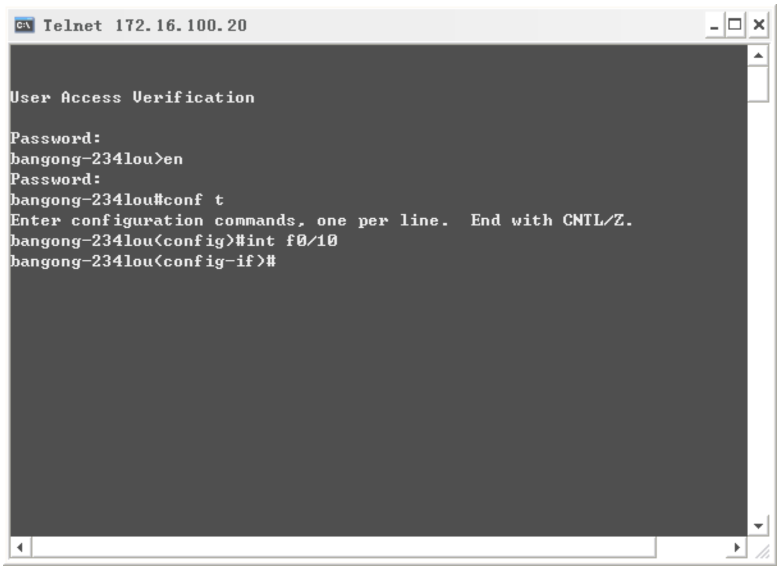


图 5-30　命令的简略方式

5. 使用 no 命令

使用 **no**，可建立一个 no 结构的命令。no 结构命令可完成下列任务。

命令将其恢复至默认值。如：用 speed 命令修改端口的速率之后，使用 no speed 命令，可恢复端口的默认速率。

no 结构命令也可执行命令的相反活动。如：使用 **shutdown** 命令关闭 interface 后，使用 **no shutdown** 命令，则执行与其相反的动作，即重新开启该 interface，如图 5-31 所示。

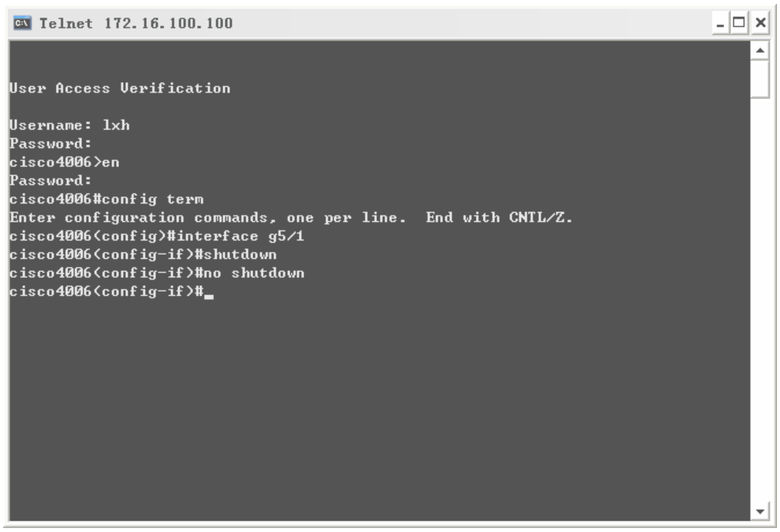


图 5-31　no 命令

6. 理解命令行出错信息

在使用 CLI 配置交换机时，可能会显示一些出错信息，表 5-2 中给出了这些出错信息的含

义，解决的方法则是键入空格后再键入？以显示完整的命令，然后再照葫芦画瓢。

表 5-2　出错信息的含义

出错信息	含　义
% Ambiguous command: "show con"	需要键入足够长的字符，以便于交换机能够识别该命令，也就是说，您的命令太过简略了，以至于与其他命令有前半部分相同，从而导致交换机不能识别和执行
% Incomplete command.	没有键入全部的关键字或参数值
% Invalid input detected at `^' marker.	键入的命令不正确，符号^指出了错误所在

7. 命令行约定

在具体的配置过程中，会反复显示命令格式，以及交换机和路由器的输出信息。为了使大家能够正确区分其不同含义，特做如下约定。

■ **命令描述中的约定**

- 命令和关键字使用**粗体**字。
- 需要由使用者根据具体情况进行修改的参数使用*斜体*字。
- 拥有两个或两个以上关键字，但每次只能够选择一个的关键字被置于{}中，并使用|将其分割开来。
- 可选的关键字和参数被置于[]中。

■ **示例中的约定**

- 终端会话或系统显示的信息使用**黑体**字。
- 键入的信息使用**粗体**字。

5.2.2 指定端口、VLAN、MAC 和 IP

1. 指定端口

当指定特定端口时，其命令语法为：

```
port_type mod_num/port_num
```

即端口类型 模块号/端口号

例如，Fastethernet 3/1 表示位于模块 3 上的端口 1，该端口类型为快速以太网。

■ **端口类型**

交换机端口类型主要包括以下几种：

- Ethernet　10 Mbps 端口
- FastEthernet　100 Mbps 端口
- GigabitEthernet　1000 Mbps 端口
- TenGigabitEthernet　10 Gbps 端口

■ **模块化交换机**

模块化交换机都在插槽位置标明插槽号（如图 5-32 所示），并在模块上标明端口号。通常

情况下，模块的排序为从上到下，顶端为 1；端口的排序为从左至右，左侧为 1。

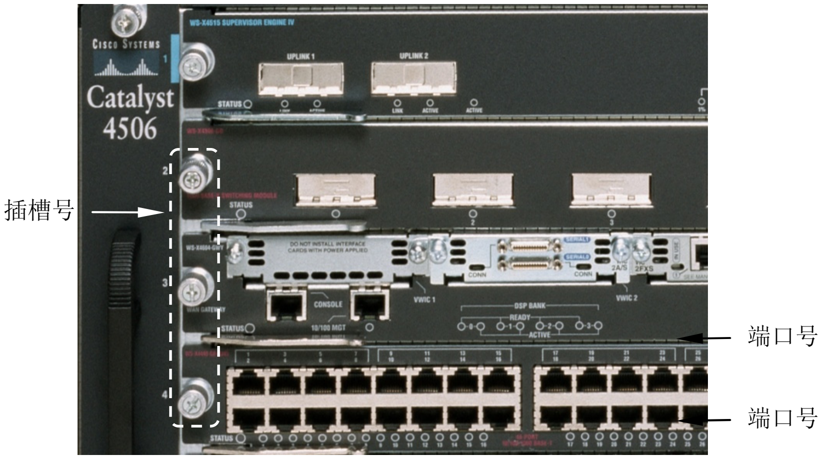


图 5-32　模块号

例如，位于 Catalyst 4506 第 3 插槽中的是拥有 24 个 1000Base-T 端口的线卡，那么，当描述该线卡第 8 个端口时，应当使用 GigabitEthernet 3/8，或者简称 g 3/8。再如，位于 Catalyst 6509 第 4 个插槽中的是拥有 6 个 10 Gbps 插槽的线卡，那么，当描述该线卡第 3 个插槽或端口时，应当使用 TenGigabitEthernet 4/3，或者简称 t 4/3。

■　**固定端口交换机**

同样，固定配置交换机也标明有端口号（如图 5-33 所示）。通常情况下，固定配置交换机（Catalyst 3750 系列除外）上的所有端口都位于 0 模块上。

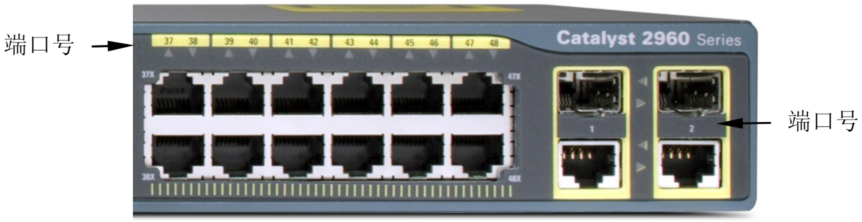


图 5-33　端口号

例如，当描述 Catalyst 2960 第 10 个快速以太网端口时，应当使用 FastEthernet 0/10，或者简称 f 0/10。而描述 Catalyst 2960 第 1 个千兆位以太网端口时，应当使用 GigabitEthernet 0/1，或者简称 g 0/10。

Catalyst 3750 系列交换机采用“1/0/端口号”的方式来描述端口。例如，描述 Cayalyst 3750G 的第 9 个千兆位以太网端口时，应当使用 GigabitEthernet 1/0/9，或者简称 g 1/0/9。而描述第 1 个万兆位以太网端口时，应当使用 TenGigabitEthernet 1/0/1，或者简称 t 1/0/1。

■　**端口列表**

为了快速配置多个端口，可以指定一个端口范围，即端口列表，从而为这些端口配置相同的参数和功能。在指定端口列表时，使用逗号，可指定一个单独的端口，使用连字符“-”可指定端口范围（两个号码之间的所有端口）。连字符优先于逗号。

指定端口或端口范围示例如下：

3/4-8　　　指定插槽 3 上的端口 4 至端口 8

5/2,5/4,6/10　　　指定插槽 5 上的端口 2 和端口 4，及插槽 6 上的端口 10

3/1-3,4/8　　　指定插槽 3 上的端口 1 至端口 3，及插槽 4 上的端口 8

当然，在指定端口范围时，必须同时指定其端口类型。例如，指定 Catalyst 2960 的快速以太网端口 1 至端口 9 时，应当使用 FastEthernet 0/1-9，简称 f 1-9。指定 Catalyst 3750G 的千兆位以太网端口 1 至端口 9 时，应当使用 GigabitEthernet 1/0/1-9，简称 g 1/0/1-9。

2. 指定 VLAN

在 VLAN 加上一个数字即为 VLAN ID，用于识别 VLAN。在指定 VLAN 列表时，使用逗号，（不能插入空格）可指定一个单独的 VLAN，使用连字符“-”可指定 VLAN 范围（两个号码之间的所有 VLAN）。

指定 VLAN 或 VLAN 范围的示例如下：

8　　　指定 VLAN 10

2,5,8　　　指定 VLAN 2、VLAN 5 和 VLAN 8

2-9,12　　　指定 VLAN 2 至 VLAN 9，及 VLAN 12

3. 指定 MAC 地址

在命令中指定 MAC（Media Access Control）地址时，必须使用标准格式。MAC 地址必须是以连字符分开的 6 个十六进制数，如下所示：

```
00-00-e8-66-86-b7
```

4. 指定 IP 地址信息

在命令中指定 IP 地址时，必须使用点分十进制格式。如下所示：

```
192.168.8.80
```

在命令中指定子网掩码时，可以使用点分十进制格式，也可以采用数字方式直接表示掩码的位数。如下所示：

```
255.255.255.0
```

也可直接表示为子网掩码的位数，如 24。

5.3 交换机初始化配置

交换机的基本配置主要包括交换机的初始化配置、SNMP 配置和端口配置，为交换机指定管理 IP 地址信息及用户名和密码，以保证能够实现对交换机的远程管理。因此，在交换机分发之前，必须对交换机进行初始化。

5.3.1 图形界面初始化配置

可网管交换机应当在完成基本配置后，再将其安装至相应的网络位置。首次设置交换机

时，应当使用快速设置输入初始 IP 信息，使交换机能够连接至本地路由器和因特网。然后，可以在日后配置时通过此 IP 地址访问交换机。

Cisco Catalyst 2950/2960/3550/3560/3750/3650/3850 等系列交换机可采用以下方式，实现基本参数的快速设置。

① 确认没有任何设备连接至交换机。在快速设置期间交换机作为 DHCP 服务器使用。如果配置用计算机设置有静态 IP 地址，在开始操作之前，应将其设置为“自动获得 IP 地址”方式。

② 将交换机连接至正确接地的交流电插座，大致 30 s 之后开始加电自检（POST，Power-on Self-test），完成整个过程大致需要 5 min。在 POST 期间，一系列测试证实交换机正常工作时，SYSTEM LED 指示灯将呈绿色并闪烁，XPS、STATUS、DUPLEX 和 SPEED LED 指示灯呈绿色并常亮。交换机完成 POST 后，SYSTEM LED 指示灯呈绿色，MAST LED 指示灯也呈绿色（如果该交换机作为主堆叠交换机），其他 LED 指示灯熄灭。如果交换机的 POST 失败，SYST LED 指示灯将变成琥珀色，或者呈绿色并闪烁。

提·示 POST 期间 LED 的行为是不可预见的，且可能各有不同。POST 错误通常是致命的。如果交换机的 POST 失败，立即致电给 Cisco 网络产品经销商。

③ 按住模式（MODE）按钮（可能需要 3 s 以上），直至模式按钮所有 LED 指示灯都变为绿色时，松开模式按钮，交换机将进入快速设置（Express Setup）模式。

提·示 如果在按下按钮之后，模式按钮上方的 LED 开始闪烁，松开按钮。闪烁的 LED 说明交换机配置已经完成，不能进入快速设置模式。某些型号交换机上的 RPS LED 始终是熄灭状态。

④ 使用超五类直通线，将计算机网卡与交换机前面板上的任何一个 10/100 Mbps、10/100/1000 Mbps 端口或者 MGMT 端口连接在一起，确认网卡和相应交换机端口上的 LED 指示灯都已变为绿色。

提·示 智能交换机的端口在连接其他设备时（如计算机或其他交换机），首先呈琥珀色，即阻止该端口的连接。当确认该连接没有导致拓扑环时，该端口才变为绿色，此时方可通信。

⑤ 等待大致 30 s 时间。

提·示 如果端口 LED 指示灯没有在 30 s 之后变为绿色，应当确认：

- 双绞线跳线所连接的是交换机访问端口，而不是 Console 端口。
- 使用的是良好的超五类或六类双绞线跳线，并且是直通线。
- 其他设备打开了电源。

⑥ 在计算机上启动 Web 浏览器，在“地址栏”中输入 IP 地址“10.0.0.1”，并按 Enter 键，

显示如图 5-34 所示的快速设置页面。默认密码是“cisco”。

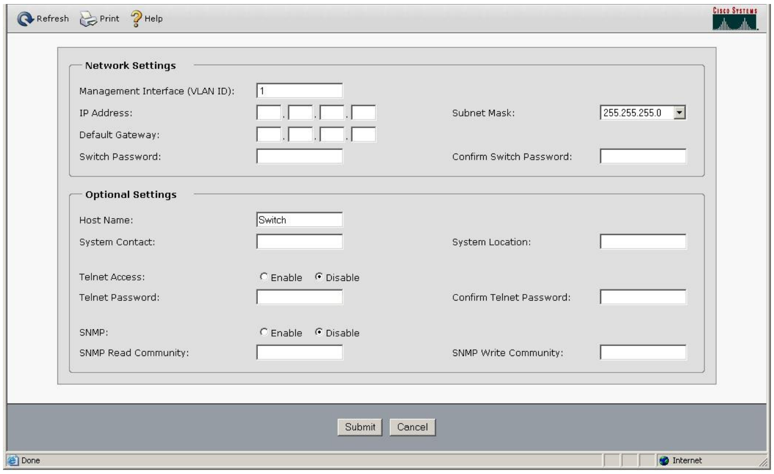


图 5-34　快速设置页面

提·示　虽然不同型号交换机的配置界面略有不同，不过，大多数配置参数还是大致相同的。如果快速设置窗口未能显现，确认 Web 浏览器上的“弹出窗口阻止程序”或者“代理服务器”设置未被启用，并且在计算机上禁用了无线客户端。

⑦ 在“Network Settings”网络设置选项组中，输入有关交换机管理的重要信息。

- Management Interface（VLAN ID）：在管理接口（VLAN ID）字段中默认值为 1。只有在用户想要更改管理接口（通过该接口管理交换机，且将 IP 信息分配给该接口）时，输入新的 VLAN ID。VLAN ID 范围为 1～1001。
- IP Address：在 IP 地址文本框中输入该交换机的管理 IP 地址。
- Subnet Mask：在子网掩码下拉列表中选择子网掩码。
- Default Gateway：在默认网关文本框中输入默认网关（路由器）的 IP 地址。
- Switch Password：在交换机密码文本框中输入 Enable 密码。密码为 1～25 个字母和数字的组合，可以数字开始，区分大小写，允许内嵌空格。但空格不容许位于开始或结尾处。除核心交换机和重要位置的交换机外，建议为所有交换机设置相同的密码，以便于进行统一管理。
- Confirm Switch Password：在确认交换机密码文本框中再次输入密码。

注·意　所有输入必须均为英文字母和数字。

⑧（可选）在“Optional Settings”选项组中输入可选设置信息，也可稍后使用设备管理器接口输入。

- Host Name：在主机名文本框中输入该交换机名称，用于与其他交换机相区别。主机

名限于 31 个字符，不允许内嵌空格。交换机名称建议包括交换机型号、位置、功能、编号等相关消息，便于该交换机与其他交换机相区分。

- System Contact：在系统联系人文本框中输入交换机负责人的姓名。
- System Location：在系统位置文本框中输入交换机所位于的布线室、楼层或建筑物。
- Telnet Access：如果想要通过命令行接口（CLI）使用远程登录来管理交换机，在远程登录访问字段中选中“Enable”单选按钮；如果启用了远程登录访问，必须输入远程登录密码。
- Telnet Password：在远程登录密码字段中输入密码。远程登录密码为 1～25 个字母和数字的组合，区分大小写，允许内嵌空格，但空格不容许位于开始或结尾处。
- Confirm Switch Password：再次输入远程登录密码。
- SNMP：在 SNMP 字段中选中“Enable”单选按钮，启用简单网络管理协议（SNMP）。只有当计划使用 CiscoWorks、Cisco CNA、HP OpenView，或者其他基于 SNMP 的网络管理系统来管理交换机时，才建议启用 SNMP 功能。
- SNMP Read Community/SNMP Write Community：如果启用了 SNMP，必须在 SNMP 读取团体字符串字段，或者 SNMP 写入团体字符串字段，或者在这两个字段中输入团体字符串。

提·示 SNMP 团体字符串验证对 MIB 对象的访问。SNMP 团体字符串中不允许存在内嵌空格。设置 SNMP 读取团体字符串时，可以访问 SNMP 信息，但是不得修改。设置 SNMP 写入团体字符串时，可以访问并修改 SNMP 信息。

⑨ 单击“Submit”按钮，提交保存设置。单击提交时，交换机配置完成并退出快速设置模式。

提·示 配置用计算机将显示一条警告信息，然后试图连接至新的交换机 IP 地址。如果使用与个人计算机中不同子网的 IP 地址配置交换机，个人计算机和交换机之间的连接性就会丢失。

⑩ 将交换机与配置计算机断开，然后根据既定的设计方案，将交换机安装在网络中适当的位置。

5.3.2 对话式初始配置

将采用 Console 端口连接至交换机后，交换机第一次加电运行时，将显示初始化配置信息。在对话式的字符交互界面下，可以完成对交换机参数的基本配置。

例如，初始化配置 Catalyst 2950 交换机，将其主机名设置为 Wangluo_2960，管理 IP 地址为 172.16.100.3，子网掩码为 255.255.255.0，enable 密码为 Coolpen，Enable 加密密码为 Coolpen.net，Telnet 密码为 Coolpen.net。SNMP 参数稍后再进行配置。

① 键入“yes”，进入初始配置对话模式。

Would you like to enter the initial configuration dialog? [yes/no]: ***yes***

At any point you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity

for management of the system, extended setup will ask you

to configure each interface on the system.

② 键入“yes”，进入基本管理配置。

Would you like to enter basic management setup? [yes/no]: ***yes***

③ 为交换机键入名称并按 Enter 键。主机名最多为 28 字符，成员交换机最多为 31 个字符。任何交换机不能使用-n（n 为数字）作为主机名的最后字符。

Enter host name [Switch]: ***Wangluo_2960***

④ 键入 eanble secret 密码并按 Enter 键。密码为 1～25 个字符（字母或数字），可以数字开始，对大小写敏感，允许使用空格，但第一个字符是空格时无效。secret password 密码被加密，不能正常显示。enable 密码可以正常显示。

Enter enable secret: ***Coolpen***

⑤ 键入 enable 密码并按 Enter 键。密码要求与 eanble secret 相同。

Enter enable password: ***Coolpen.net***

⑥ 键入虚拟终端（如 telnet）密码并按 Enter 键。密码要求与 eanble secret 相同。

Enter virtual terminal password: ***Coolpen.net***

⑦ 键入“no”，稍后再以 CLI 命令行、Cisco CNA 或其他管理软件配置 SNMP（Simple Network Management Protocol）。

Configure SNMP Network Management? [no]: ***no***

⑧ 键入连接到管理网络的接口名称（物理接口或 VLAN 名称）并按 Enter 键。通常情况下，使用 VLAN1 作为管理接口。

Enter interface name used to connect to the

management network from the above interface summary: ***vlan1***

⑨ 为交换机指定 IP 地址和子网掩码并按 Enter 键。

Configuring interface vlan1:

Configure IP on this interface? [yes]: ***yes***

IP address for this interface: ***172.16.100.3***

Subnet mask for this interface [255.0.0.0]: ***255.255.255.0***

⑩ 键入“y”，将交换机配置为群集命令交换机。键入“n”，则将其配置为成员交换机或独立交换机。可以稍后借助 CLI 等方式进行配置，此处键入“n”。

Would you like to enable as a cluster command switch? [yes/no]: ***no***

至此，已经完成了该交换机的初始化配置，并显示配置概览。

The following configuration command script was created:

hostname Wangluo_2060

enable secret 5 1Ulq8$DlA/OiaEbl90WcBPd9cOn1

enable password Coolpen

line vty 0 15

```
password Coolpen
no snmp-server
!
no ip routing
!
interface Vlan1
no shutdown
ip address 172.16.100.3 255.255.255.0
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
interface GigabitEthernet1/0/3
!
…<output abbreviated>
!
interface GigabitEthernet1/0/23
interface GigabitEthernet1/0/24
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Choose (2) to save the configuration to NVRAM to use it the next time the switch reboots.
Enter your selection [2]:2
```

选择“2”保存配置并退出。

5.3.3 CLI 命令初始化配置

当然，能够图形化配置的交换机也可以使用 CLI 命令行进行快速地初始化。若欲使交换机可远程管理，必须为其指定 IP 地址信息和名称。另外，还应当为交换机指定新的管理密码。若欲使其可被网管软件管理，还应当指定 SNMP 字符串。

> **提·示** 对于中高端交换机（如 Cisco Catalyst 4500 和 Catalyst 6500 系列）而言，只能使用 CLI 命令行以纯手工方式初始化配置交换机。

■ **配置命令**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为交换机指定新的名称。

```
Switch(config)# hostname name
```

③ 为特权模式指定新的密码。

```
Switch(config)# enable password password
```

或者，指定新的 enable 加密密码。当设置加密密码后，非加密 enable 密码将不再可用。

```
Switch(config-line)#enable secret secret_password
```

④ 进入 VTY Line 模式，配置 Telnet 远程访问密码。

```
Switch(config)# line vty 0 15
```

⑤ 为 Telnet 指定新的访问密码。

```
Switch(config-line)# password password
```

⑥ 返回全局访问模式。

```
Switch(config-line)# exit
```

⑦ 进入 CON Line 模式，配置 Console 端口访问密码。

```
Switch(config)# line con 0
```

⑧ 为 Console 端口访问指定新的密码。

```
Switch(config-line)# password password
```

⑨ 返回全局访问模式。

```
Switch(config-line)# exit
```

⑩ 进入 VLAN1。交换机的管理 VLAN 为 VLAN1，因此为交换机指定 IP 地址信息时，也必须进入 VLAN1 中进行配置。

```
Switch(config)# interface vlan 1
```

⑪ 键入为该交换机指定用于远程管理的 IP 地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

⑫ 激活并启用 VLAN1。

```
Switch(config-if)# no shutdown
```

提·示

该步骤是必需的，否则，将由于 VLAN1 没有被激活而无法实现对该交换机的远程管理。

⑬ 返回全局访问模式。

```
Switch(config-line)# exit
```

⑭（可选）为交换机指定默认网关。通常情况下，默认网关为核心层交换机的管理 IP 地址。

```
Switch(config)# ip default-gateway IP-address
```

提・示 二层交换机配置管理 IP 地址后，在与管理计算机同 IP 网段内，可以直接使用“Telnet *ip_address*”命令登录并连接。但是，若欲跨网段登录并连接到其他网段的二层交换机，就必须给二层交换机配置指定默认网关。对于三层交换机，则不需要配置管理地址和默认网关地址，可使用三层交换机上的任何一个三层接口的 IP 地址来远程登录。

⑮ 指定 SNMP 通知主机的 IP 地址。

```
Switch(config)# snmp-server host ipaddress | hostname
```

⑯ 设置 SNMP 只读或读写字符串。

```
Switch(config)# snmp-server community string [ro | rw]
```

⑰ 启用 SNMP 陷阱。

```
Switch(config)# snmp-server enable traps
```

提・示 如果网络内没有设置 SNMP 网管软件，则 SNMP 相关参数不必进行配置，否则，将徒增网络内的流量。当然，SNMP 参数也可以在稍后通过远程网络重新进行配置。

⑱ 二层交换机配置了管理 IP 地址后，在管理地址的同网段内，就可利用“Telnet 192.168.1.254”来登录连接到交换机了。但若要跨网段去登录连接到另一个网段的二层交换机，则必须给二层交换机配置指定默认网关，双方的二层交换机都要配置指定默认网关地址。配置指定交换机的默认网关地址使用 ip default-gateway 命令。对于三层交换机，则不需要配置管理地址和默认网关地址，可使用三层交换机上的任何一个三层接口的 IP 地址来远程登录。

⑲ 返回特权配置模式。

```
Switch(config)# exit
```

⑳ 校验键入的信息是否正确。

```
Switch# show running-config
```

㉑ 保存配置。如果不保存，在交换机重新启动时，修改的配置将全部丢失。

```
Switch# copy running-config startup-config
```

至此，交换机的基本管理信息配置完成。

> **提·示** 有关密码和字符的相关要求，请参见“5.3.2 对话式初始配置”。

■ **配置示例**

初始化配置 Catalyst 4506 交换机，将其主机名设置为 Hexin_4506，管理 IP 地址为 172.16.100.1，子网掩码为 255.255.255.0，enable 密码为 Coolpen，Telnet 密码为 Coolpen.net。SNMP 参数稍后再进行配置。

```
Switch> enalbe
Switch# configure terminal
Switch(config)# hostname Hexin_4506
Hexin_4506 (config)# enable password Coolpen
Hexin_4506 (config)# line vty 0 15
Hexin_4506 (config-line)# password Coolpen.net
Hexin_4506 (config)# line con 0
Hexin_4506 (config-line)# password Coolpen.net
Hexin_4506 (config)# interface vlan 1
Hexin_4506 (config-if)# ip address 172.16.100.1 255.255.255.0
Hexin_4506 (config-if)# no shutdown
Hexin_4506 (config-if)# end
Hexin_4506 # show running-config
Hexin_4506 # copy running-config startup-config
```

再如，初始化配置 Catalyst 2960 交换机，将其主机名设置为 Network_2960，管理 IP 地址为 172.16.100.100，子网掩码为 255.255.255.0，默认网关为 172.16.100.1，enable 密码为 Coolpen，Telnet 密码为 Coolpen.net。SNMP 参数稍后再进行配置。

```
Switch> enalbe
Switch# configure terminal
Switch(config)# hostname Network_2960
Network_2960 (config)# enable password Coolpen
Network_2960 (config)# line vty 0 15
Network_2960 (config-line)# password Coolpen.net
Network_2960 (config)# line con 0
Network_2960 (config-line)# password Coolpen.net
Network_2960 (config)# interface vlan 1
Network_2960 (config-if)# ip address 172.16.100.100 255.255.255.0
Network_2960 (config-if)# no shutdown
Network_2960 (config-if)# exit
Network_2960 (config)# ip default-gateway 172.16.100.1
Network_2960 (config)# end
Network_2960 # show running-config
Network_2960 # copy running-config startup-config
```

第 6 章　使用 CLI 配置交换机

使用 CLI 命令行配置交换机，虽然难度较大，但是，却可以实现较为复杂的设备配置。事实上，许多功能和参数只能借助 CLI 方式进行配置。因此，是否熟悉和掌握 CLI 命令行，是衡量技术人员水平的重要标准之一。另外，交换机和路由器的 CLI 命令行基本相同。可见，CLI 对于配置和管理网络设备是非常重要的。

6.1　交换机配置前的规划

搭建网络时，通常情况下，都是先在网络中心统一配置好交换机，然后，再分发到各楼宇的机柜中安装。因此，在动手配置交换机前，必须做好统筹和规划工作，避免可能产生的 IP 地址、名称等各种冲突和混乱。所有规划都必须制作为电子文档，以备配置时参考和日后查看。

■ **IP 地址规划**

IP 地址的规划包括以下几个方面的内容。

- 选择网络内使用的 IP 地址范围。如果合法 IP 地址数量较少，建议采用 192.168.0.0～192.168.255.255 或 10.0.0.0～10.255.255.255 段的私有 IP 地址。
- 为每个 VLAN 指定不同的 IP 地址范围，并确定其子网掩码和默认网关，便于为该 VLAN 的计算机分配 IP 地址信息。
- 为每台交换机指定管理使用的 IP 地址信息，便于实现对该交换机的远程管理。

■ **名称规划**

名称规划包括以下几个方面的内容。

- 每个端口所连接计算机的名称，用于确认该交换机所连接的计算机，便于日后实现对该端口的远程管理。
- 每台交换机的名称，用于确认该交换机所处的位置，便于与其他交换机区分，并对该交换机实现远程管理。
- 每个 VLAN 的名称，用于确认该 VLAN 的性质，便于与其他 VLAN 区分，并实现对该 VLAN 的管理。

■ **安全规划**

安全规划包括以下几个方面的内容。

- VLAN 的划分，即将哪些部门划分至同一 VLAN，每个 VLAN Trunk 允许哪些 VLAN 通过和访问，以及在哪些交换机上设置哪些 VLAN。
- PVLAN，确定将哪些端口设置为 PVLAN 端口，用于禁止端口之间的相互通信，并借助访问列表实现三层访问控制，从而确保该端口所连接计算机的安全。

- 安全访问列表，确定在哪些交换机上使用哪些访问列表，用于禁止在某个时间段访问网络、禁止访问某些 TCP 或 UDP 端口、禁止使用某些 IP 协议、限制某些 IP 地址范围内计算机的网络访问权限等。
- 安全端口，确定将哪些交换机上的哪些端口设置为安全端口，用于限制连接某个端口的 MAC 地址，以避免非授权计算机访问网络；或者限制某个端口所允许的 MAC 地址数量，以禁止用户私自级联集线设备接入计算机。
- IEEE 802.1x 认证，确定是否采用身份认证的方式实现网络访问安全，以及安全认证服务器如何搭建与配置。
- 传输控制，在哪些端口启用基于端口的传输控制，以保证网络的正常运行，避免可能产生的网络拥塞。

■ **堆叠规划**

堆叠规划包括以下几个方面的内容。

- 哪些交换机以堆叠方式实现相互连接，是否拥有必要的堆叠模块。
- 采用何种方式实现堆叠连接，冗余连接方式还是非冗余连接方式，全带宽模式还是半带宽模式。
- 对叠堆如何管理，采用单一 IP 地址管理，还是分别管理。

■ **功能规划**

功能规划主要包括以下几个方面的内容。

- EtherChannel，确定是否采用 EtherChannel 来增加网络带宽、提供链接冗余和负载均衡，在哪些网络设备的哪些端口之间的连接上采用 EtherChannel。
- PortFast，确定是否采用 PortFast 减少计算机连接网络的时间，避免长时间的等待。
- QoS，确定是否采用 QoS，以保证视频会议等即时信息的无阻塞传输。
- 多播，确定是否采用多播，以减少网络流量，节约网络带宽。规划并分配多播的 IP 地址。

6.2 配置 VLAN

VLAN 配置大致可以分为 4 个步骤，即设置 VTP 服务器/客户端，创建 VLAN，将端口指定至 VLAN，创建 VLAN 中继。一般情况下，VTP 服务器被配置于核心层交换机，而汇聚层交换机和接入交换机则充当 VTP 客户端角色。

6.2.1 VTP 版本和配置策略

借助 VTP 设置，可以只在 VTP 服务器上创建、删除和管理 VLAN，而不必在每台交换机上都重复创建和管理 VLAN 的操作，从而既保证了全局 VLAN 的统一性，也减少了 VLAN 维护的复杂性。因此，对于较大规模的网络而言，采用 VTP 进行 VLAN 配置和管理是必要的，也是必需的。

> **提·示**
> 在交换机配置之前，应当确保已经对交换机进行了初始化。有关交换机初始化的操作技术，请参见“第 5 章 交换机配置方式与初始化”。

1. VTP 配置策略

在网络中执行 VTP 时，应当遵守下述策略。

- 配置 VTP 时，必须配置一个 Trunk 端口，以确保交换机能够向/从其他交换机发送/接收 VTP 通告。
- VTP 信息保存在 VTP VLAN 数据中。当 VTP 模式是透明时，VTP 域名和模式被保存于交换机 running configuration 文件中，可以使用 copy running-config startup-config 命令，将其保存于 startup configuration 文件。若欲在交换机重新启动时，交换机仍然保存为 VTP 透明模式，则必须执行上述命令。
- 当在 startup configuration 文件中保存 VTP 模式，并且重新引导交换机时，交换机配置选择下列之一：
    - 如果 startup configuration 中 VTP 模式是透明模式，并且 VLAN 数据库、VTP 域名与 startup configuration 文件相匹配，VLAN 数据库将被忽略（清除），使用 startup configuration 文件中的 VTP 和 VLAN 配置。VLAN 数据库中的 VLAN 数据库修订号不会改变。
    - 如果 startup configuration 中 VTP 模式或域名与 VLAN 数据库不匹配，域名、VTP 模式和 VLAN ID 使用 VLAN 数据库中的信息配置。
- 当第一次配置 VTP 时，必须为其指定域名。同时，必须为 VTP 域中所有的交换机指定相同的域名。处于 VTP 透明模式中的交换机不会与其他交换机交换 VTP 消息，也无需为其配置 VTP 域名。

> **提·示**
> 如果 NVRAM 和 DRAM 存储空间足够，处于 VTP 域中的所有交换机都将处于 VTP 服务器模式。如果所有交换机都运行于 VTP 客户端模式，就不能配置 VTP 域。即使配置域，也不能在域中使修改的 VLAN 配置生效。因此，应当确认在 VTP 域中至少配置了一台 VTP 服务器。

- 可以为 VTP 域配置密码，但是，并不是必须的。如果配置了域密码，所有域交换机必须共享相同的密码，并且必须在管理域内的每一台交换机上配置该密码。没有配置密码，或者配置错误的密码，交换机将拒绝 VTP 通告。

> **提·示**
> 当配置 VTP 密码后，如果不为域中的每台交换机都分别指定一个管理域密码，管理域将不能实现全部功能。

- 在 VTP Server 上启用或禁用 VTP 修剪将导致整个管理域启用或禁用 VTP 修剪。

- 如果将交换机配置为 VTP 客户端模式，交换机将不能创建 VLAN 数据库文件（vlan.dat）。当交换机关闭电源并重新启动时，将重置 VTP 为默认配置。若欲在交换机重新启动后依然保持 VTP 客户端的 VTP 配置，必须配置 VTP 域名。

2. VTP 版本

- 一个 VTP 域中的所有交换机必须使用相同的域名，但是，无需相同的 VTP 版本。
- 在同一 VTP 域中，如果能够执行 VTP 版本 2 的交换机没有启用版本 2，也就是说，版本 2 是被禁用的，那么它将被视为运行 VTP 版本 1 的交换机。版本 2 默认被禁用。
- 如果交换机运行 VTP 版本 1，但是能够运行 VTP 版本 2，在接收到 VTP 版本 3 通告后，能够自动改变为 VTP 版本 2。
- 如果运行 VTP 版本 3 交换机连接至运行 VTP 版本 1 交换机，VTP 版本 1 交换机改变为 VTP 版本 2，VTP 版本 3 交换机发送缩小版本的 VTP 包，使 VTP 版本 2 交换机能够更新数据库。
- 当配置有扩展 VLAN 时，运行版本 3 的交换机不能改变为版 1 或 2。
- 除非同一 VTP 域中的所有交换机都能够执行 VTP 版本 2，否则，不应当在交换机上启用 VTP 版本 2。当在一台交换机上启用 VTP 版本 2 时，同一域中的所有能够运行版本 2 的交换机都将启用版本 2。如果有只能运行版本 1 的交换机，将不能与其他启用版本 2 的交换机交换 VTP 信息。
- Cisco 推荐在网络边缘使用 VTP 版本 1 和 2 交换机，因为它们不能转发 VTP 版本 3 通告。
- VTP 版本 1 和 2 不能传播扩展 VLAN（VLAN 1006～4094）的配置信息，必须在每台设备上手工配置这些 VLAN。VTP 版本 3 支持扩展 VLAN 数据库传播。
- VTP 版本 3 设备不会发送 VTP 版本 2 格式包，除非在中继端口接收到 VPT 版本 2 包。也就是说，当在 VTP 版本 3 设备的中继端口接收到 VTP 版本 2 设备的消息时，将发送一个 VTP 版本 2 格式的 VLAN 数据库。
- 当 VTP 版本 3 设备在中继端口发现 VTP 版本 2 设备时，除继续发送 VTP 版本 3 包外，还将在中继端口附加发送 VTP 版本 2 包。
- VTP 版本 3 设备不接受来自 VTP 版本 2 或版本 1 设备的配置信息。

3. VTP 默认配置

VTP 配置默认值如表 6-1 所示。

表 6-1 VTP 配置默认值

功　　能	默 认 值
VTP 域名	空
VTP 模式	Server
VTP 版本 2 可用状态	Version 2 禁用
VTP 版本 3 可用状态	Version 3 禁用
VTP 密码	无
VTP 修剪	禁用

6.2.2 配置 VTP

汇聚层交换机和接入交换机应当配置为 VTP 客户端并加入 VTP 域，以实现网络管理员对 VLAN 的统一管理。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 配置 VTP 管理域名。名称为 1～32 个字符。只有拥有相同域名的 VTP 服务器和客户端才可被统一管理。

```
Switch（config）# vtp domain domain-name
```

③ 将交换机配置为 VTP 服务器/客户端/透明模式，或关闭 VTP。当将交换机添加为 VTP 客户端时，通常需要校验其 VTP 配置版本号是否低于同一 VTP 域中的其他交换机。VTP 域中的交换机通常使用 VTP 版本号较高的交换机中的 VLAN 配置。对于版本 1 和版本 2 来说，当向域中添加高版本的交换机时，可能会从 VTP 服务器和 VTP 域中删除所有的 VLAN 信息。对于 VTP 版本 3 而言，则 VLAN 信息不会被删除。

```
Switch（config）# vtp mode ｛ server | client | transparent | off ｝
```

> **提示** 对于小型网络而言，如果不想采用“VTP 域+VTP 客户端”的方式，也可以将所有交换机设置为 VTP 透明模式。这样，就需要在每台交换机上分别创建 VLAN，然后，再将相应的端口指定至所属的 VLAN。当然，也将无法实现对网络内 VLAN 的统一管理。

将版本 3 VTP 服务器由默认的次要服务器改变为主要服务器。其中，vlan 表明选择使用 VLAN 数据库接管，mst 表明选择使用 MST（Multiple Spanning Tree，多扩展树）接管，force 表明覆盖任何有冲突的配置。如果没有 force 关键字，将被提示确认是否接管。

```
Switch（config）# vtp primary [ vlan | mst] [ force]
```

④ 设置 VTP 域密码。密码长度为 8～64 个字符。

```
Switch（config）# vtp password password
```

> **提示** 若欲取消 VTP 域密码，可以使用 no vtp password 全局配置命令。
> 若欲禁用 VTP 修剪，可以使用 no vtp pruning 全局配置命令。

⑤（可选）在交换机上启用 VTP 版本 1/2/3。默认状态下，VTP 版本 2/3 被禁用。

```
Switch（config）# vtp version ｛ 1 | 2 |3 ｝
```

⑥（可选）在 VTP 管理域中启用 VTP 修剪。默认状态下，从 VLAN 2 到 VLAN 1000 均可修剪。VLAN 1 通常不可被修剪。

```
Switch# vtp pruning
```

⑦ 返回至特权配置模式。

```
Switch（config）#end
```

⑧ 查看并校验 VTP 版本号、状态和配置。

```
Switch# show vtp status
```

⑨ 保存 VTP 配置。

```
Switch# copy running-config startup-config
```

> **提·示**
> 在交换机引导时，如果 startup-config 和 vlan.dat 文件中的 VTP 域名和 VTP 模式不匹配，交换机将使用 vlan.dat 文件中的配置引导。

6.2.3 创建和管理 VLAN

VLAN 的主要作用有两点，一是提高网络安全性，阻止未经授权的 VLAN 访问，二是提高网络传输效率，将广播隔离在子网之内。因此，VLAN 划分是可网管交换机最基本的配置之一。

1. VLAN 配置文件

VLAN 1～1005 的配置被写入 vlan.dat 文件（VLAN 数据库），可以在特权模式下使用 show vlan 命令查看 VLAN 相关信息。文件 vlan.dat 存储于闪存中。如果 VTP 模式为透明，也被保存于交换机的运行配置文件（running-configuration）。

在接口配置模式下，可以将端口从 VLAN 中添加或移除。这些命令被写入运行配置文件，可以使用 show running-configuration 查看。

当在启动配置文件（startup-configuration）中保存 VLAN 和 VTP 信息（包括扩展 VLAN 配置信息），并重新引导交换机。交换机配置将从下述项目中选择：

- 如果启动配置中 VTP 模式为透明，VLAN 数据库与启动配置文件中的 VTP 域名相匹配，VLAN 数据库被忽略（清除），使用启动文件中的 VTP 和 VLAN 配置信息。VLAN 数据库中的 VLAN 数据库修订号不改变。
- 如果启动配置文件中的 VTP 模式或域名与 VLAN 数据库不匹配，的 VTP 域名、VTP 和 ID 为 1～1005 的 VLAN，使用 VLAN 数据库信息进行配置。
- VTP 版本 1 和 2，如果 VTP 模式为服务器，域名和 VLAN 1～1005 使用 VLAN 数据库信息配置。VTP 版本 3 也支持 VLAN 1006～4094。

2. 标准 VLAN 配置策略

VLAN 1～1005 为标准 VLAN。在创建和修改标准 VLAN 时，应当遵循以下策略。

- 在 VTP 客户端、服务器和透明模式中，交换机支持 1005 个 VLAN。
- 标准 VLAN 的 ID 号为 1～1001。VLAN 号为 1002～1005 的是 Token Ring 和 FDDI VLAN。
- VLAN 1～1005 通常被保存在 VLAN 数据库中。如果 VTP 模式是透明的，VTP 和 VLAN 配置也保存在交换机运行配置文件中。
- 如果交换机处于 VTP 服务器或 VTP 透明模式，可以在 VLAN 数据库中添加、修改或移除 VLAN 2～1001。VLAN 1 和 VLAN 1002～1005 将自动创建，并不能移除。
- 在创建 VLAN 之前，交换机必须处于 VTP 服务器模式或 VTP 透明模式。如果交换机是 VTP 服务器，必须定义 VTP 域。
- 交换机支持 128 个生成树实例。如果交换机有太多的活动 VLAN，超过所支持的扩展树，扩展树将在 128 个 VLAN 启用，并且禁用其他的 VLAN。如果已经在交换机上使用了所有可用的扩展树实例，无论在 VTP 域何处添加 VLAN，那么，该交换机将不运行扩展树。如果在该交换机的中继端口有默认允许列表（允许所有 VLAN），新 VLAN 将在所有中继端口传输，在某些拓扑结构的局域网中，可能会导致环路而瘫痪。
- 当堆叠中的交换机学习新 VLAN，或者删除、修改原有 VLAN 时，VLAN 信息会传播给堆叠中的所有成员。
- 当交换机加入堆叠或堆叠混合时，新交换机上的 VTP 信息（vlan.dat 文件）将与活动交换机并存。

3. 扩展 VLAN 配置策略

VLAN 1006～4094 是扩展 VLAN。在创建扩展 VLAN 时，应当遵循下述策略：

- 在 VTP 透明模式下，创建的扩展 VLAN 不保存在 VLAN 数据库中，并且不能扩散。在 VTP 服务器模式下，VTP 版本 3 支持扩展 VLAN（VLAN 1006～4094）数据库的扩散。
- 扩展 VLAN 不被保存在 VLAN 数据库中，并且对 VTP 无效，除非在 VTP 版本 3 交换机中。
- VTP 版本 1 和 2，可以在全局模式下配置 VTP 模式为透明。需要将该配置保存至启动配置中，以便交换机以 VTP 透明模式引导。否则，交换机重新加载时，将丢失扩展 VLAN 配置。如果在 VTP 版本 3 中创建了扩展 VLAN，不能将其转变为 VTP 版本 1 或 2。
- 当交换机上拥有最大数量的扩展树实例时，在任何新创建的 VLAN 中扩展树都将被禁用。如果交换机上的 VLAN 数量超过了扩展树实例的最大值，推荐配置 MSTP（Multiple STP，多扩展树），从而将多个 VLAN 映射至一个扩展树实例。
- 在交换机堆叠中，所有成员使用相同的启动配置和保存配置，扩展 VLAN 信息可以穿越堆叠而被共享。

4. VLAN 默认配置

以太网 VLAN 默认配置和范围如表 6-2 所示。

表 6-2 以太网 VLAN 默认配置和范围

属　性	默　认	有 效 值
VLAN ID	1	1～4094。扩展范围 VLAN（ID 6～4094）不能被保存在 VLAN 数据库
VLAN 名称	VLANxxxx，其中 xxxx 表示为与 VLAN ID 相同的数字，包括 0 开头的 VLAN ID	没有范围
IEEE 802.10 SAID	100001（100000 加 VLAN ID）	1～4294967294
MTU 大小	1500	1500～18190
VLAN 状态	活动	活动，挂起，禁用

5. 创建 VLAN

创建 VLAN 共需要两个步骤，先是创建 VLAN，再将相关接口指定至该 VLAN。这个过程相似于先划分若干部门，然后再将人员一一分配至不同部门。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 键入 VLAN ID，进入 VLAN 配置模式。以太网 VLAN ID 的取值范围为 1～1001。其中，VLAN 1 为系统默认 VLAN，不能被创建，也不能被删除。

```
Switch(config)# vlan vlan_id
```

提示：如果键入的 VLAN ID 不存在，那么，此时将自动创建该 VLAN。因此，首次进入某个 VLAN 的过程，也是创建该 VLAN 的过程。

③ 为 VLAN 命名，便于区分、查看和管理 VLAN。如果不为 VLAN 命名，默认在 VLAN ID 前添加 0 作为 VLAN 名称。例如，VLAN0004 是 VLAN 4 的默认名称。

```
Switch(config-vlan)# name vlan-name
```

提示：为 VLAN 命名后，使用 show vlan 命令，可以方便地查看该 VLAN 所属的部门或用户群，便于对 VLAN 进行后期的配置和管理，因此，建议为每个 VLAN 命名。

④ 返回全局配置模式。

```
Switch(config-vlan)# exit
```

提示 若欲创建多个 VLAN，并将端口指定至 VLAN，必须一一重复执行上述命令。

⑤ 查看并检验 VLAN 配置。

```
Switch# show vlan [id | name] vlan_name
```

⑥ 保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

6. 将端口指定至相应的 VLAN

指定欲配置至该 VLAN 的接口。创建 VLAN 之后，接下来就需要根据规划将相应的端口指定至该 VLAN。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置的端口或端口范围。

```
Switch(config)# interface interface-id
```

或

```
Switch(config)# interface range interface-range
```

提示 若欲将多个端口指定至同一 VLAN，建议采用指定端口组的方式，一次将多个端口指定至同一 VLAN。

③ 在配置完成之前禁用该端口。

```
Switch(config-if)# shutdown
```

④ 将接口配置二层交换接口。在使用其他带有关键字的 switchport 命令之前，必须使用不带任何关键字的 switchport 命令一次，以将该接口作为二层接口。或者，以前在该接口上使用过 no switchport 命令，也必须使用该命令。

```
Switch(config-if)# switchport
```

⑤ 将该接口指定为二层访问模式。

```
Switch(config-if)# switchport mode access
```

注意 在将交换机端口指定至某个 VLAN 之前，必须将该端口设置为二层接口。尤其是对于三层交换机而言，默认状态下，所有接口都是三层接口，因此，将指定端口设置为二层交换端口就显得更为必要。

⑥ 将该端口指定至相应的 VLAN。

```
Switch(config-if)# switchport access vlan vlan_id
```

⑦ 重新激活该接口，使其恢复转发状态。

```
Switch(config-if)# no shutdown
```

⑧ 退出接口配置状态。

```
Switch(config-if)# end
```

⑨ 查看该接口的运行状态。

```
Switch# show running-config interface interface-id
```

⑩ 显示该接口的交换端口配置。

```
Switch# show interfaces interface-id switchport
```

⑪ 保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

提·示 若欲将多个端口指定至不同 VLAN，必须一一重复执行上述命令。当然，不能将一个端口指定至多个 VLAN。当将一个端口指定至一个新的 VLAN 后，该端口将只属于新指定的 VLAN。

7. 管理 VLAN

提·示 如果交换机处于 VTP 透明模式，VLAN 配置被保存在运行配置文件时，也被保存至 VLAN 数据库。这里只是将当前配置保存至启动配置。

■ 删除指定 VLAN

使用 **no vlan** vlan_id 命令，可删除指定的 VALN。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 删除指定的 VLAN。

```
Switch(config-vlan)# no vlan vlan_id
```

③ 更新 VLAN 数据库，并返回特权配置模式。

```
Switch(config-vlan)# end
```

④ 校验 VLAN 的改变。

```
Switch(config-vlan)# show vlan brief
```

⑤ 保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

提示 删除 VLAN 后，所有指定至 VLAN 的端口将不再可用，直到将其指定至新 VLAN 时止。若欲一次性删除所有创建的 VLAN，则必须借助删除 vlan.dat 数据库的方式。

■ **清除接口配置**

将指定接口恢复为默认值，即可清除该接口的所有配置，当然也包括 VLAN 设置。

① 进入 VLAN 配置模式。

```
Switch# config terminal
```

② 清除某接口的所有配置。

```
Switch(config)# default interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port
```

③ 返回特权配置模式。

```
Switch(config)# end
```

④ 保存对配置的修改。

```
Switch# copy running-config startup-config
```

提示 若欲将接口指定至其他 VLAN，只需直接将其指定至新 VLAN ID 即可，而不必先清除接口配置再指定至新 VLAN。

6.2.4 配置中继

当在交换机上划分有多个 VLAN 时，若欲借助一条链路实现与其他交换机的通信，就必须创建 Trunk（中继）。默认状态下，第二层接口自动处于动态的 Switchport 模式，当相邻接口（即借助于双绞线或光纤连接在一起的两个端口）支持 Trunk，并且配置为 Trunk 或动态匹配模式时，该链接即可作为 Trunk 链接。

1. Trunk 封装协议与适用

可以借助 IEEE 802.1q、ISL（Inter-Switch Link Protocol，交换链路协议）和 DTP（Dynamic Trunking Protocol，动态中继协议）等 3 种不同的封装协议创建中继。

其中，802.1q 作为 IEEE 标准适用于在任意交换机之间创建中继。因此，无论是在 Cisco 交换机之间，还是在 Cisco 交换机与其他品牌的交换机创建 Trunk，802.1q 封装协议无疑都是最佳选择。

ISL 是 Cisco 私有协议，主要用于维护交换机和路由器间的通信流量等 VLAN 信息。DISL（Dynamic Inter-Switch Link Protocol，动态交换链路内协议）则简化了两台相互连接的快速以太网设备上 ISL 中继的创建过程。

DTP 用于管理 Trunk 协商，支持在 ISL 和 802.1q 中继间自动协商。

两个接口的 Trunk 模式、Trunk 封装类型和硬件能力决定了连接创建为 ISL 中继还是 802.1q 中继。

以太网 Trunk 封装类型如表 6-3 所示。

表 6-3　以太网 Trunk 封装类型

封装类型	封装命令	描　　述
ISL	switchport trunk encapsulation isl	在 Trunk 链路上指定 ISL 封装
802.1q	switchport trunk encapsulation dot1q	在 Trunk 链路上指定 802.1q 封装
Neighboring	switchport trunk encapsulation negotiate	指定接口与相邻接口协商，根据相邻接口的配置和能力，创建 ISL 或 802.1q 中继

Cisco Catalyst 交换机平台支持的中继协议如表 6-4 所示。

表 6-4　Cisco Catalyst 交换机平台支持的中继协议

平　　台	802.1Q	ISL	DTP
Catalyst 6500/6000	是	是	是
Catalyst 5500/5000	是	是	是
Catalyst 4900/4500/4006	是	是	是
Catalyst 3750/3850	是	是	是
Catalyst 3650/3560/3550	是	是	是
Catalyst 2970	是	是	是
Catalyst 2960	是	否	是
Catalyst 2950/2955	是	否	是
Catalyst 2940	是	否	是
Catalyst 2948G-L3/4908G-L3/4840G	是	是	否
Catalyst 8500	是	是	否

二层接口模式及其相应的特性如表 6-5 所示。

表 6-5　二层接口模式及其相应的特性

模　　式	特　　性
switchport mode access	将接口（访问端口）置于永久性非 Trunk 模式，并且协商将链路转换至非 Trunk 链路。即使相邻接口是 Trunk 接口，接口也将改变为非 Trunk 接口
switchport mode dynamic auto	接口能够转换链路为 Trunk。当相邻接口设置为 Trunk 或 desirable 模式时，接口将改变为 Trunk 接口。所有以太网接口的默认 switchport 模式都是 dynamic auto
switchport mode dynamic desirable	接口能够积极尝试将链路转换为 Trunk。当相邻接口设置为 trunk、desirable 或 auto 模式时，接口将改变为 Trunk 接口
switchport mode trunk	将接口置于永久性 Trunk 模式，并协商将相邻链路转换为 Trunk 链路。即使相邻接口不是 Trunk 接口，接口也将改变为 Trunk 接口
switchport nonegotiate	阻止发出 DTP 协商的接口。将接口置于 Trunk 模式。只有当接口 switchport 模式是 access 或 trunk 时，才能使用该命令。必须手动配置相邻接口为 Trunk 接口，以建立 Trunk 链路

2. Trunk 上允许的 VLAN

默认状态下，Trunk 端口允许所有 VLAN 的发送和接收通信。所有 VLAN，从 1 到 4094，在每个中继接口都被允许通信。当然，根据需要，也可以从访问列表中移除某些 VLAN，拒绝这些 VLAN 通过 Trunk 传输，从而限制该 VLAN 与其他交换机的通信，或者拒绝某些 VLAN 对敏感数据的访问。

为了避免生成树环或广播风暴，可以在某些特殊 VLAN 中继的允许列表中移除 VLAN1。当从 Trunk 端口移除 VLAN1 时，接口将继续发送和接收管理通信，如 CDP （Cisco Discovery Protocol，Cisco 发现协议）、PAgP（Port Aggregation Protocol，端口聚合协议）、LACP（Link Aggregation Control Protocol，链路聚合控制协议）、DTP 等，同时，VTP 也在 VLAN 1 中。因此，一般情况下，不建议从 Trunk 中移除 VLAN1。

VLAN1 被禁用的 Trunk 端口转换为非 Trunk 端口时，将添加该访问 VLAN。如果访问 VLAN 被设置为 1，端口将添加 VLAN1，而不管 switchport trunk allowed 如何设置。端口上被禁用的所有 VLAN 都是如此。

如果 VTP 知道该 VLAN，并且该 VLAN 在端口的允许访问列表中，那么，当 VLAN 被启用时，则 Trunk 端口可以改变为 VLAN 成员。当 VTP 发现一个新启用的 VLAN，并且该 VLAN 在 Trunk 端口的允许访问列表中时，该 Trunk 端口将自动改变为该新启用 VLAN 的成员。当 VTP 发现一个新 VLAN，并且 VLAN 没在 Trunk 端口的允许访问列表时，该 Trunk 端口不能改变为该新启用 VLAN 的成员。

3. 二层以太网接口默认配置

二层以太网接口默认配置如表 6-6 所示。

表 6-6 二层以太网接口默认配置

特 性	默 认 值
接口模式	switchport mode dynamic auto
Trunk 封装	switchport trunk encapsulation negotiate
允许 VLAN 范围	VLAN 1–1005
VLAN 修剪合格范围	VLAN 2–1001
默认 VLAN（访问端口）	VLAN 1
本地 VLAN（802.1Q 中继）	VLAN 1
STP	在所有 VLAN 启用
STP 端口优先级	128
STP 端口开销	10 Mbps 端口为 100 10/100 Mbps 端口为 19 100 Mbps 端口为 19 1000 Mbps 端口为 4 10 000 Mbps 端口为 2

4. Trunk 配置策略

在配置 Trunk 时，应当遵循以下策略或限制。

- 在由 Cisco 交换机连接创建的 IEEE 802.1q 中继中，交换机将为中继所允许的每个 VLAN 都保持一个实例，而非 Cisco 设备只支持一个扩展树实例（为所有 VLAN）。

借助 802.1q 中继连接 Cisco 交换机和非 Cisco 交换机时，Cisco 交换机合并非 Cisco 交换机扩展树实例。

- 确认 Trunk 所连接的两端 IEEE 802.1q 中继的本地 VLAN 是相同的。如果两端的本地 VLAN 不同，可能会导致扩展树环。
- 建议不启用 Trunk 中的本地 VLAN 的扩展树，或者在网络中的每个 VLAN 中禁用扩展树。在禁用扩展树前，一定要确认网络中不存在拓扑环。
- Trunk 端口不能是安全端口。
- Trunk 端口可以是 EtherChannel 端口组的成员，但是，该 EtherChannel 组中的所有 Trunk 必须使用相同的配置。当 EtherChannel 组第一次创建时，所有端口的下述参数将被设置为添加至该组的第一个端口的相应参数。如果修改其中任何一个端口的参数，交换机都会将该改变扩散至该组中的其他所有端口。

① 允许 VLAN 列表。

② 每个 VLAN 的 STP 端口优先级。

③ STP Port Fast 配置。

④ Trunk 状态。如果端口组中的一个端口停止作为 Trunk，所有端口都将停止作为 Trunk。

- 在 PVST（Per VLAN Spanning Tree，每 VLAN 生成树）模式中，建议最多配置 24 个 Trunk 端口；在 MST（Multiple Spanning Tree，多生成树）模式中，建议最多配置 40 个 Trunk 端口。
- 如果尝试在 Trunk 端口上启用 IEEE 802.1x，将会收到一个错误消息提示，并且 IEEE 802.1x 不会生效；如果尝试将已经启用 IEEE 802.1x 的端口修改为 Trunk，端口模式也不会改变。
- 动态端口可以与相邻端口协商而改变为 Trunk 端口。如果在动态端口上尝试启用 IEEE 802.1x，将会收到一个错误消息提示，并且 IEEE 802.1x 不会生效；如果尝试将已经启用 IEEE 802.1x 的端口修改为动态端口，端口模式也不会改变。

5. 配置 Trunk 端口

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲设置为 Trunk 的接口。当然，Trunk 应当在交换机级联端口上配置。

```
Switch(config)# interface interface_id
```

③ 在配置完成之前禁用该端口。

```
Switch(config-if)# shutdown
```

④ 指定 Trunk 采用的封装模式。建议选择使用 dot1q 封装，以获得最大的兼容性。

```
Switch(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}
```

⑤ 将接口配置为第二层 Trunk。dynamic auto，是指如果相邻接口被设置为 trunk 或 desirable 模式，将该接口设置为 Trunk 连接。dynamic desirable，是指如果相邻接口设置为 trunk、desirable 或 auto 模式，将该接口设置为 Trunk 连接。trunk，是指将接口设置为永久 Trunk 模

式，即使相邻接口不是 Trunk 接口，也会与之协商将连接转换为 Trunk 连接。建议相邻接口均使用 trunk 关键字，以保证 Trunk 创建成功。

```
Switch(config-if)# switchport mode {dynamic {auto | desirable} | trunk}
```

> **提·示** 只有接口是第二层访问接口，或者指定 Trunk 模式时，才需要使用该命令。

⑥（可选）指定默认 VLAN，即当 Trunk 失效后，允许哪一个 VLAN 使用 Trunk 链路继续通信。既可指定某一个 VALN，也可以指定一个 VLAN 范围。访问 VLAN 不能作为本地 VLAN 使用。

```
Switch(config-if)# switchport access vlan vlan_id
```

⑦（可选）为 802.1q Trunk 指定本地 VLAN。若不指定本地 VLAN，默认将使用 VLAN1。

```
Switch(config-if)# switchport trunk native vlan vlan_id
```

⑧ 配置 Trunk 上允许的 VLAN 列表。使用 add（添加）、all（所有）、except（除外）和 remove（移除）关键字，可以定义允许在 Trunk 上传输的 VLAN。VLAN 列表既可以是一个 VLAN，也可以是一个 VLAN 组。当同时指定若干 VLAN 时，不要在“,”或“-”间使用空格。

```
Switch(config-if)# switchport trunk allowed vlan {add | all | except | remove}
vlan-list
```

⑨ 重新启动指定接口。

```
Switch(config-if)# no shutdown
```

⑩ 返回至特权配置模式。

```
Switch(config-if)# end
```

⑪ 查看并校验配置。

```
Switch# show interface interface_id switchport
Switch# show interfaces interface_id trunk
```

⑫ 保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

若欲将接口恢复至默认值，可以使用 default interface *interface_id* 接口配置命令。若欲将 Trunk 接口中的所有特征恢复为默认值，可以使用 no switchport trunk 接口配置命令。若欲禁用 Trunk，可以使用 switchport mode access 接口配置命令，端口将作为一个静态访问端口。

若欲允许所有 VLAN 都通过该 Trunk，可以使用 **no switchport trunk allowed vlan** 接口配置命令。

提·示 Trunk应当在相互连接的两台交换机上分别设置，否则Trunk将无法生效。也就是说，当在接入交换机的级联端口上设置了Trunk端口后，还应当在汇聚层交换机的相应端口上设置Trunk。同时，在汇聚层交换机上必须创建Trunk中所包含的全部VLAN ID。

6.3 配置链路冗余

对于大中型网络而言，为了保证网络的稳定性与可靠性，链路的冗余是必需的。然而，链路冗余也意味着拓扑环路，从而导致网络通信瘫痪。因此，正确配置链路冗余，并消除可能存在的环路，是保证网络高效、可靠通信的关键。

6.3.1 配置PVST

对于交换机而言，首先应当解决的就是可能的拓扑环问题。原因很简单，导致拓扑环的原因非常多，无论是误将一条跳线连接在同一交换机的两个端口，还是跳线短路，或者将交换机拓扑连接为环路，都会导致拓扑环的发生，从而导致网络瘫痪。

1. STP默认配置参数

STP默认配置参数如表6-7所示。

表6-7 STP默认参数配置

特　征	默认设置
启用状态	VLAN1启用，最多可以启用64个STP
扩展树模式	PVST+（Rapid PVST+和MSTP被禁用）
交换机优先级	32768
STP端口优先级	128
STP端口开销	1000 Mbps: 4 100 Mbps: 19 10 Mbps: 100
STP VLAN端口优先级	128
STP VLAN端口开销	1000 Mbps: 4 100 Mbps: 19 10 Mbps: 100
扩展树计时器	Hello时间：2 s 转发延迟时间：15 s 最大老化时间：20 s 发送保持计数：6BPDU

提·示 若欲重新启用STP，可以使用**spanning-tree vlan** *vlan_id*全局配置命令。

2. 配置根交换机

默认状态下，所有 VLAN 中的扩展树都将启用 PVST+。对于中小型网络而言，VPST+是一个不错的选择，因此，无需再为每个 VLAN 都启用 STP，只需将核心层交换机确定为根交换机即可。

当 VLAN 中存在有拓扑环时，应当通过根交换机设置确定网络拓扑结构，从而使扩展树的生成时间最短。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将交换机配置为指定 VLAN 的根交换机。使用 *vlan_id* 可以指定某个 VLAN 或 VLAN 范围，可取值范围为 1～4094。（可选）**diameter** net- diamete 用于指定两个终端间交换机的数量，取值范围为 2～7。使用 **spanning-tree vlan** *vlan_id* **root secondary [diameter** net- diamete 命令，可以将交换机配置为次根交换机。（可选）使用 **hello-time** *seconds*，指定来自根交换机配置信息的时间间隔，单位为秒，可取值范围为 1～10，默认值为 2。

```
Switch(config)# spanning-tree vlan vlan_id root primary [diameter net- diameter
[hello-time seconds]]
```

③ 返回至特权配置模式。

```
Switch(config)# end
```

④ 查看并校验配置。

```
Switch# show spanning-tree detail
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

若欲将交换机恢复为默认配置，可以在全局配置模式下使用 **no spanning-tree vlan** *vlan_id* **root** 命令。

3. 配置次根交换机

如果网络中还有第二台核心层交换机，那么，也可以同时配置一台次根交换机。当交换机作为次根交换机时，在指定 VLAN 中，该交换机的优先级将由默认的 32 768 被修改为 28 672。当指定 VLAN 中的根交换机失败后，该交换机将非常容易地改变为根交换机。而网络中其他优先级为 32768 的交换机则将很难改变为根交换机。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将交换机配置为指定 VLAN 的次根交换机。相关参数请参见 STP 根交换机配置。

```
Switch(config)# spanning-tree vlan vlan_id root secondary [diameter net-
diameter [hello-time seconds]]
```

③ 返回至特权配置模式。

```
Switch(config)# end
```

④ 查看并校验配置。

```
Switch# show spanning-tree detail
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

若欲将交换机恢复为默认配置，可以在全局配置模式下使用 **no spanning-tree vlan** *vlan_id* **root** 命令。

6.3.2 配置 MSTP

STP/RSTP 协议以及 Cisco 的私有协议 PVST+都属于单生成树（Single Spanning Tree，SST）协议，也就是对于支持多 VLAN 的设备只能运行单一的生成树。MSTP 是 IEEE 802.1s 中提出的一种 STP 和 VLAN 结合使用的新协议，既继承了 RSTP 端口快速迁移的优点，又解决了 RSTP 中不同 VLAN 必须运行在同一个生成树上的问题。可见，如果网络内的交换机全部支持 MST 协议，则应当尽量配置为 MST。

1. MSTP 默认配置参数

MSTP 默认配置参数如表 6-8 所示。

表 6-8 MSTP 默认配置参数

特　　性	默认配置
扩展树模式	PVST+ (Rapid PVST+和 MSTP 被禁用)
交换机优先级	32768
扩展树端口优先级	128
扩展树端口开销	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello 时间	2 s
转发延迟时间	15 s
最大老化时间	20 s
最大步跳计数	20

2. MSTP 配置策略

配置 MSTP 时，应当遵循以下策略。

- 当使用 spanning-tree mode mst 全局配置命令启用 MST 时，RSTP 被自动启用。
- 若欲使 2 台或更多交换机位于同一 MST 区域，必须拥有相同的 VLAN-实例映射、相同配置版本号和相同的名称。
- 交换机支持最多 65 个 MST 实例。不过，被映射至某一 MST 实例的 VLAN 数量没有限制。
- PVST+、Rapid PVST+和 MSTP 都被支持，但是，在任何时候都只能激活一个版本。例如，所有 VLAN 运行 PVST+，或者所有 VLAN 运行 rapid PVST+，或者所有 VLAN 运行 MSTP。

- MST 配置中的 VTP 传播不被支持。不过，可以在 MST 区域中的每台交换机上手动配置 MST 配置（如区域名称、版本号和 VLAN-实例映射）。
- 在网络中，可以借助冗余路径实现负载分担，所有 VLAN-实例映射必须匹配，否则，所有传输流量将只使用其中的一条链路。
- 所有 MST 边界端口必须为 PVST+和 MST 云或者 rapid-PVST+和 MST 云之间的负载分担转发。
- 不建议将网络划分为较多数量的区域。然而，如果这种情况不可避免，建议将交换式网络划分为较小局域网，并借助路由器或非二层设备互连。

> **注·意**
> 不能在网络中同时启用 MSTP 和 PVST。对于中小型网络而言，不妨使用 PVST 协议实现扩展树算法。

3. MSTP 基本配置

① 进入全局配置模式。

```
Switch# configure terminal
```

② 进入 MST 配置模式。

```
Switch(config)# spanning-tree mst configuration
```

③ 映射 VLAN 至 MST 实例。实例 ID 取值范围为 0～4094，VLAN 取值范围为 1～4094。当将 VLAN 映射至 MST 实例时，在映射增加的同时，指定的 VLAN 也将从早先的映射中添加或移除。若欲指定一个 VLAN 范围，可以使用“-”连字符，如“instance 1 vlan 1-11”将把 VLAN1～VLAN11 映射至 MST 实例 1；若指定一个 VLAN 系列，则可以使用“,”，如“instance 1 vlan 10, 20, 30”将把 VLAN10、VLAN20 和 VLAN30 映射至 MST 实例 1。

```
Switch(config-mst)# instance instance_id vlan vlan-range
```

④ 指定配置名称。名称字符串最多允许 32 个字符。

```
Switch(config-mst)# name name
```

⑤ 指定配置版本号。取值范围为 0～65535。

```
Switch(config-mst)# revision version
```

⑥ 查看并校验配置。

```
Switch(config-mst)# show pending
```

⑦ 确认对配置所做的修改，并返回至全局配置模式。

```
Switch(config-mst)# exit
```

⑧ 启用 MSTP。RSTP 也将被启用。不能同时运行 MSTP 和 PVST+或者 MSTP 和 rapid PVST+。

```
Switch(config)# spanning-tree mode mst
```

⑨ 返回特权配置模式。

```
Switch(config)# end
```

⑩ 查看并校验配置。

```
Switch# show running-config
```

⑪ 保存修改的配置。

```
Switch# copy running-config startup-config
```

4. 配置根交换机

交换机维护一个 VLAN 组的扩展树实例映射。交换机 ID 由交换机优先级和交换机 MAC 地址组成，并被关联到每个实例。对于某个 VLAN 组而言，交换机 ID 最低的交换机将变为根交换机。

通过将核心层交换机配置为根交换机确定网络拓扑结构，从而使扩展树的生成时间最短。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将交换机配置为根交换机。使用 *instance_id* 既可指定单个实例，也可指定一个实例范围，取值范围为 0～4094。（可选）**diameter** net- diamete 用于指定两个终端间交换机的数量，取值范围为 2～7。该关键字只在 MST 实例 0 中有效。（可选）使用 **hello-time** *seconds*，指定来自根交换机配置信息的时间间隔，单位为秒，可取值范围为 1～10，默认值为 2。

```
Switch(config)# spanning-tree mst instance_id root primary [diameter net-diameter [hello-time seconds]]
```

③ 返回至特权配置模式。

```
Switch(config-mst)# end
```

④ 查看并校验配置。

```
Switch# show spanning-tree mst instance_id
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

若欲将交换机恢复为默认配置，可以在全局配置模式下使用 **no spanning-tree vlan** *vlan_id* **root** 命令。

5. 配置次根交换机

可以将交换机配置为次根交换机，从而使其优先级由默认的 32768 修改为 28672。在指定的实例中，当根交换机失败后，该交换机将非常容易地改变为根交换机。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将交换机配置为指定实例的次根交换机。相关参数请参见 MST 根交换机配置。

```
Switch(config)# spanning-tree mst instance_id root secondary [diameter net-diameter [hello-time seconds]]
```

③ 返回至特权配置模式。

```
Switch(config-mst)# end
```

④ 查看并校验配置。

```
Switch# show spanning-tree detail
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

若欲将交换机恢复为默认配置，可以在全局配置模式下使用 **no spanning-tree mst** instance_*id* **root** 命令。

6.3.3 配置链路汇聚

使用 PAgP 或 LACP 协议，可以很容易地在有 EtherChannel 能力的端口间自动建立 Fast EtherChannel、Gigabit EtherChannel 和 TenGigabit EtherChannel 连接，实现数据通信与转发。LACP 协议具有学习相邻端口组动态和信息的能力。PAgP 是 EtherChannel 的增强版，支持在 EtherChannel 上的 Spanning Tree 和 Uplink Fast 功能，并支持自动配置 EtherChannel 捆绑。

> **提·示** 只有在固定端口（如双绞线端口或光纤端口）之间才能创建 EtherChannel，而由 GBIC 或 SFP 插槽所创建的链路是不能用于创建 EtherChannel 的。

1. EtherChannel 模式与构建

■ **EtherChannel 模式**

可以将 EtherChannel 配置为以下任何一种模式：Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)或 On。配置 EtherChannel 两端为同一模式。

- 当配置 EtherChannel 的一端为 PAgP 或 LACP 模式时，系统将协商另一端以确定端口是否改变为活动（active）。如果远程端口不能协商为 EtherChannel，本地端口将进入自主状态，并向其他单独的链路一样继续传输数据。虽然端口配置不会改变，但是，端口也不能加入至 EtherChannel。
- 当配置 EtherChannel 的一端为 on 模式时，协商不会发生。交换机将强制 EtherChannel 中的所有兼容端口改变为活动。链路汇聚中的另外一端（在其他交换机上）必须也配置为 on 模式，否则，将可能会导致包丢失。

① EtherChannel LACP 模式

- active，激活接口的主动协商状态，通过发送 LACP 包与其他接口进行主动协商。
- passive，当侦测到 LACP 设备时，将只启用 LACP。将端口置于被动协商状态，可以对接收到的 LACP 作出响应，但不能主动发送 LACP 包进行协商。该设置将发送最

少的 LACP 包。

- on，将接口强行指定至 Channel，无论是 PAgP 还是 LACP。不过，只有当两个 on 模式接口组连接时，EtherChannel 才可用。

> **提·示**
> LACP 能够在支持 IEEE 802.3ad 协议的设备间创建 EtherChannel。因此，当 Cisco 交换机与其他品牌的交换机之间创建端口汇聚时，应当首选 LACP 协议。

启用 active 或 passive 模式的端口与拍档协商构建 EtherChannel 时，必须基于相同的标准，如相同的端口速率、Trunk 状态和 VLAN ID。

② EtherChannel PAgP 模式

- auto，将端口置于被动协商状态，可以对接收到的 PAgP 作出响应，但不能主动发送 PAgP 包进行协商。该设置将发送最少的 PAgP 包。
- desirable，无条件启用 PAgP。将接口置于主动协商状态，通过发送 PAgP 包，主动与其他接口进行协商。该模式支持交换机堆叠中 EtherChannel 成员位于不同交换机的情况（即跨堆叠 EtherChannel）。
- on，将接口强行指定至 Channel，无论是 PAgP 还是 LACP。只有两个 on 模式接口组连接时，EtherChannel 才可用。

> **注·意**
> 某些早期型号的交换机和早期版本的 Cisco IOS 不支持 LACP 模式。因此，当在不同型号和不同 Cisco IOS 版本的交换机之间配置 EtherChannel 时，采用 PAgP 协议不失为一种好的选择。当然，由于 LACP 协议可以容纳更多端口数量的，因此，当相邻交换机都支持 LACP 时，应当尽量采用 LACP 协议创建。

在 auto 或 desirable 模式下，交换机端口只在拍档端口之间交换 PAgP 包。端口配置为 on 模式时，则不会交换 PAgP 包。

启用 auto 或 desirable 模式的端口与拍档协商构建 EtherChannel 时，必须基于相同的标准，如相同的端口速率、Trunk 状态和 VLAN ID。

■ EtherChannel 构建模式

采用 LACP 协议时，即使端口处于不同的 LACP 模式，只要模式相互兼容，也同样能构建 EtherChannel。以下模式可以构建 EtherChannel：

- 一个接口为 active 模式，另一个接口为 active 或 passive 模式。

> **提·示**
> 当采用 LACP 协议时，相邻接口均采用 Active 模式将确保能够创建 EtherChannel。

当一个端口处于 passive 模式时，不能与另外一个处于 passive 模式的端口构建 EtherChannel，因为两个端口都不会开始 LACP 协商。

采用 PAgP 协议时，即使端口处于不同的 PAgP 模式，只要模式相互兼容，也同样能构建 EtherChannel。以下几种模式可以构建 EtherChannel：

- 一个接口为 desirable 模式，另一个接口为 desirable 或 auto 模式。
- 一个接口为 auto 模式，另一个接口为 desirable 模式。

> **提示**
> 当采用 PAgP 协议时，相邻接口均采用 desirable 模式将确保能够创建 EtherChannel。

当一个端口处于 auto 模式时，不能与另外一个处于 auto 模式的端口构建 EtherChannel，因为两个端口都不会开始 PAgP 协商。

2. EtherChannel 配置策略

EtherChannel 配置策略和限制如下：

- Catalyst 3850 在交换机堆叠上最多可以创建 128 个 Etherchannel，Catalyst 3750 在交换机堆叠上最多可以创建 48 个 Etherchannel，Catalyst 3560 在交换机堆叠上最多可以创建 48 个 Etherchannel，Catalyst 2960 在交换机堆叠上最多可以创建 6 个 EtherChannel。
- PAgP EtherChannel 最多容纳 8 个相同类型的以太网接口。
- LACP EtherChannel 最多容纳 16 个相同类型的以太网接口。最多 8 个端口被激活，最多 8 个端口处于备用模式。
- Catalyst 3750 可以跨堆叠配置由 2 个 10-Gigabit 模块端口创建的 EtherChannel。
- 对于模块交换机而言，所有模块上的所有以太网接口都支持 EtherChannel，不要求这些接口必须位于同一模块上并且相邻。对于堆叠交换机而言，EtherChannel 不必来自于同一台交换机，只要是堆叠中的交换机即可。
- 必须将 EtherChannel 中的所有接口配置为相同的速率和双工模式，同时必须全部为二层接口或三层接口。
- 不能一个端口配置为一个以上的 EtherChannel 组成员。
- 不能将 EtherChannel 同时配置为 PagP 和 LACP 模式。不过，执行 PagP 和 LACP 协议的 EtherChannel 组可以在一台交换机上或同一堆叠中的不同交换机上同时运行。就特定的 EtherChannel 组而言，既可运行 PagP，也可运行 LACP，但是，两者不能同时共存。
- 必须启用 EtherChannel 中的所有接口。当其中的一个接口处于 down 状态时，该链路将处于失败状态，相应的数据将从该 EtherChannel 中的其他链路传输。
- 不能将安全端口配置为 EtherChannel，反之亦然。
- 不能将 EtherChannel 中的端口配置 IEEE 802.1x 端口。如果尝试在 EtherChannel 端口上启用 IEEE 802.1x，将会收到错误提示消息，并且 IEEE 802.1x 也不会启用。
- EtherChannel 不能来自于 SPAN（Switched Port Analyzer，交换端口分析器）目的端口。
- 对于三层 EtherChannel 而言，应当为 port-channel 逻辑接口指定 IP 地址，而不是为 EtherChannel 中的物理接口指定三层地址。

- 对于二层 EtherChannels 而言：

① 必须将 EtherChannel 中所有接口都指定至同一 VLAN，或者将其均配置为 Trunk。

② 如果从 Trunk 接口配置 EtherChannel，应当校验所有 Trunk 上的 Trunk 模式和本地 VLAN 是相同的。EtherChannel 中的接口如果使用不同的 Trunk 模式或本地 VLAN，将可能产生意想不到的结果。

③ 作为 Trunk 的二层 EtherChannel 的所有接口必须拥有相同的允许 VLAN 列表。如果选择接口所允许的范围不同，将不能构建 EtherChannel。

④ 构建 EtherChannel 的接口应当拥有相同的 STP 路径开销、STP 优先级和 Post Fast 配置。

- 配置 EtherChannel 之后，任何适用于 port-channel 接口的配置都将影响 EtherChannel；而任何适用于物理接口的配置，则将只影响接口配置。例如，Storm Control（流量控制）不能在 EtherChannel 中的部分成员上配置，必须在所有端口配置。如果只在某些端口配置，将导致 EtherChannel 接口被丢失（置于挂起状态）。因此，需要在 port-channel 接口级别（而不是在物理接口级别）配置 Storm Control。
- 只有当 EtherChannel 启用了端口安全时，启用端口安全的物理接口才能够加入二层 EtherChannel，否则，CLI 命令将被拒绝执行。
- 如果在堆叠上配置了 EtherChannel，那么，当堆叠分拆时，可能会导致拓扑环路，数据传输可能会出现问题。

> **提·示**　Catalyst 4500 系列交换机借助 EtherChannel 将最多 8 条以太网链路绑定为一个逻辑链路，与其他交换机或主机之间实现高达 1 600 Mbps（Fast EtherChannel 全双工）、16 Gbps（Gigabit EtherChannel）或 40 Gbps（10 Gigabit EtherChannel）的带宽。Catalyst 4500 最多提供 64 个 EtherChannel，每个 Etherchannel 最多可以容纳 8 个端口。

3. EtherChannel 默认配置

EtherChannel 默认配置参数如表 6-9 所示。

表 6-9　EtherChannel 默认配置参数

特　　性	默认配置
Channel 组	没有指定
Port-Channel 逻辑接口	没有定义
PAgP 模式	没有默认
PAgP 学习方法	聚合端口中在所有的接口上学习
LACP 学习方法	聚合端口中在所有的接口上学习
负载平衡	基于进入该交换机的包的源 MAC 地址进行负载分配

4. 创建 EtherChannel

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置为 EtherChannel 的物理接口或接口范围。PAgP EtherChannel 组可以容纳 8

个（4 对）同一类型和速度的端口。LACP EtherChannel 组最多可以容纳 16 个（8 对）相同类型的端口，其中 8 个（4 对）活动端口，以及最多 8 个（4 对）备用端口。

```
Switch(config)# interface interface_id
```

或者

```
Switch(config)# interface range interface-range
```

③（可选）确保没有为该接口指定 IP 地址。

```
Switch(config-if)# no ip address
```

④（可选）将指定端口设置为二层访问端口或 Trunk 端口。如果端口已经是二层访问接口或 Trunk 端口，则不必执行该操作。

```
Switch(config-if)# switchport mode {access vlan vlan_id | trunk}
```

⑤（可选）指定采用何种协议构建 EtherChannel。PAgP 是 Cisco 专有协议，LACP 是 IEEE 802.ad 标准协议。因此，若欲在 Cisco Catalyst 交换机之间创建 EtherChannel，不妨选择 PAgP；若欲在不同品牌的交换机之间创建 EtherChannel，则应当选择使用 LACP 协议。

```
Switch(config-if)# channel-protocol {lacp | pagp}
```

⑥ 将接口指定至 EtherChannel 组，并指定 PAgP 或 LACP 模式。EtherChannel 端口组的取值范围为 1～48。PAgP 协议只支持 auto 和 desirable 模式。LACP 模式只支持 active 和 passive 模式。

```
Switch(config-if)# channel-group port-channel-number mode {{auto  | desirable
| {active | passive}}
```

⑦（LACP 模式可选）指定 LACP 端口优先级，取值范围为 1～65535，默认值为 32768。较高的数字意味着较低的优先级。

```
Switch(config-if)# lacp port-priority priority_value
```

⑧ 返回特权配置模式。

```
Switch(config-if)# end
```

⑨ 查看并校验配置。

```
Switch# show running-config
```

⑩ 保存配置。

```
Switch# copy running-config startup-config
```

5. 配置 EtherChannel 负载均衡

EtherChannel 还具有负载分担和线路备份的作用。所谓负载分担，是指当交换机之间或交换机与服务器之间在进行通信时，EtherChannel 的所有链路将同时参与数据的传输，从而使所

有的传输任务都能在极短的时间内完成。这样线路占用的时间更短，网络传输的效率更高。所谓线路备份，是指当部分 EtherChannel 链路出现故障时，并不会导致连接的中断，其他链路将能够不受影响地正常工作，从而增强了网络的稳定性和安全性。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 配置 Etherchannel 负载均衡。src-mac 指源 MAC 地址；dst-mac 指目的 MAC 地址；src-dst-mac 指源和目的 IP 地址；src-ip 指源 IP 地址；dst-ip 指目的 IP 地址；src-dst-ip 指源和目的 IP 地址；src-port 指源第四层端口；dst-port 指目的第四层端口；src-dst-port 指源和目的第四层端口。其中，dst-mac 基于进入数据包的目的主机的 MAC 地址进行负载分配。在 EtherChannel 中，发送至同一目的主机的数据包被转发至相同端口，不同目的主机的数据包被发送至不同的端口。src-mac 基于进入数据包的源 MAC 地址进行负载分配。在 EtherChannel 中，来自不同主机的数据包，使用不同的端口；来自于同一主机，则使用同一端口。

```
Switch(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}
```

③ 退出全局配置模式。

```
Switch(config)# end
```

④ 校验配置。

```
Switch# show etherchannel load-balance
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

6. 管理 EtherChannel

■ 从 EtherChannel 中移除接口

① 进入配置模式。

```
Switch# configure terminal
```

② 指定欲配置的物理接口或端口范围。

```
Switch(config)# interface interface_id
```

或者

```
Switch(config)# interface range interface-range
```

③ 从 EtherChannel 中移除接口。

```
Switch(config-if)# no channel-group
```

④ 退出配置模式。

```
Switch(config-if)# end
```

⑤ 校验配置。

```
Switch# show running-config
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

■ **移除 EtherChannel**

① 进入配置模式。

```
Switch# configure terminal
```

② 移除 Channel 接口。

```
Switch(config)# no interface port-channel port_channel_number
```

③ 退出配置模式。

```
Switch(config-if)# end
```

④ 校验配置。

```
Switch# show etherchannel summary
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

6.4 配置路由

借助 Cisco IOS IP 和 IP 路由协议，核心和汇聚层交换机支持三层接口，用于实现内部网络内各逻辑网络之间的数据交换。Cisco 三层交换机提供两种类型的三层接口，即逻辑三层 VLAN 接口和物理三层接口。逻辑三层 VLAN 接口整合了路由和桥接功能，用于实现 VLAN 之间的线速路由；物理三层接口则用于连接不同类型的网络，实现不同网络之间的互联。

6.4.1 配置 SVI 接口

交换虚拟接口（Switch virtual Interface，SVI）是指在交换机上创建的 VLAN 接口。SVI 可以指定 IP 地址信息，用于实现 VLAN 间的路由交换。

> **注意**
> 在配置 SVI 接口前，必须在交换机上已经创建并配置了 VLAN，并将 VLAN 成员指定到二层接口。另外，还必须启用 IP 路由，并指定 IP 路由协议。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 创建 VLAN。如果没有创建 VLAN，使用该命令可以创建 VLAN。如果已经创建有

VLAN，则不再执行该命令。

```
Switch(config)# vlan vlan_id
```

③ 指定欲配置的 VLAN。

```
Switch(config)# interface vlan vlan_id
```

④ 为该 VLAN 指定 IP 地址和子网掩码。该 VLAN 中的计算机将使用该 IP 地址作为默认网关，以实现与其他网络的通信。

```
Switch(config-if)# ip address ip_address subnet_mask
```

⑤ 启用该 SVI 接口，否则，该 SVI 接口将处于 shutdown 状态。

```
Switch(config-if)# no shutdown
```

⑥ 返回至全局配置模式。

```
Switch(config-if)# exit
```

提·示 重复上述配置，为每个 VLAN 都指定 IP 地址信息，完成 SVI 接口的配置。

⑦（可选）如果交换机之前尚未启用 IP 路由，则必须执行该操作，以实现 VLAN 间的路由。

```
Switch(config)# ip routing
```

⑧ 返回至特权配置模式。

```
Switch(config)# end
```

⑨ 查看并校验配置。

```
Switch# show interfaces [type slot/interface]
Switch# show ip interfaces [type slot/interface]
Switch# show running-config interfaces [type slot/interface]
Switch# show running-config interfaces vlan vlan_id
```

⑩ 将配置保存至 NVRAM。

```
Switch# copy running-config startup-config
```

6.4.2 配置物理三层接口

所谓物理三层接口，是指为三层交换机的物理接口指定 IP 地址，使其成为三层路由接口。借助于物理三层接口，可以在三层交换机上实现类似传统路由的功能，实现端口间的路由。在配置物理三层接口之前，必须先启用 IP 路由，并指定 IP 路由协议。

① 进入全局配置模式。

```
Switch# configure terminal
```

② (可选)启用 IP 路由。当 IP 路由被禁用时，必须先启用 IP 路由。

```
Switch(config)#ip routing
```

③ 指定欲配置的接口。可以是物理接口，也可以是 EtherChannel。

```
Switch(config)# interface {{fastethernet | gigabitethernet} interface_id} |
{port-channel port-channel-number}
```

④ 将物理二层接口转换为物理三层接口。

```
Switch(config-if)#no switchport
```

⑤ 为该接口配置 IP 地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

⑥ 启用该物理三层接口。

```
Switch(config-if)# no shutdown
```

⑦ 退出配置模式。

```
Switch(config-if)# end
```

⑧ 校验配置。

```
Switch# show interfaces [type slot/interface]
Switch# show ip interfaces [type slot/interface]
Switch# show running-config interfaces [type slot/interface]
```

⑨ 将配置保存至 NVRAM。

```
Switch# copy running-config startup-config
```

6.4.3 配置 EtherChannel 三层接口

若欲在三层设备（如三层交换机）之间实现高速连接，可以采用三层 EtherChannel 方式，从而避免由路由连接而产生的瓶颈。当将 IP 地址从物理接口移动至 EtherChannel 时，必须先从物理接口中删除该 IP 地址。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置的物理接口。

```
Switch(config)# interface  interface_id
```

③ 创建三层路由端口。

```
Switch(config-if)# no switchport
```

④ 确保该物理接口没有指定 IP 地址。

```
Switch(config-if)# no ip address
```

⑤ 将接口配置至 port-channel，并指定 PAgP 或 LACP 模式。如果使用 PAgP 协议，使用 auto 或 desirable 关键字；如果使用 LACP 协议，使用 active 或 passive 关键字。

```
Switch(config-if)# channel-group channel-group-number mode {auto | desirable}
| {active | passive}
```

⑥ 配置 Etherchannel 负载均衡。其中，src-mac 指源 MAC 地址；dst-mac 指目的 MAC 地址；src-dst-mac 指源和目的 IP 地址；src-ip 指源 IP 地址；dst-ip 指目的 IP 地址；src-dst-ip 指源和目的 IP 地址；src-port 指源第四层端口；dst-port 指目的第四层端口；src-dst-port 指源和目的第四层端口。

```
Switch(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac |
src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}
```

⑦ 返回全局配置模式。

```
Switch(config-if)# exit
```

⑧ 选择欲配置的 port-channel 组。

```
Switch(config)# interface port-channel port_channel_number
```

⑨ 将接口置于三层模式。

```
Switch(config-if)# no switchport
```

⑩ 为该 EtherChannel 指定 IP 地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

⑪ 返回特权配置模式。

```
Switch(config-if)# end
```

⑫ 查看并校验配置。

```
Switch# show running-config interface port-channel port_channel_number
Switch# show running-config
```

⑬ 保存修改的配置。

```
Switch# copy running-config startup-config
```

6.4.4 配置三层子接口

所谓子接口，是指在单个物理接口或 Port Channel 上配置多个子接口，为用户提供很高的灵活性。借助子接口，可以在一个物理接口上支持多个逻辑接口或网络互连，即将多个逻辑接口与一个物理接口建立关联。这些逻辑接口在工作时，虽然共用物理接口的物理配置参数，但

是，各有各自的链路层和网络层配置参数。由于是多个虚接口对应一个物理接口，因此，常被称为“子接口”。

提·示 只有 Cisco Catalyst 6500 系列交换机才支持三层子接口（Subinterface），而包括 Catalyst 4500/4900 系列在内的其他三层交换机都不支持该特性。

■ **配置策略和限制**

在配置三层子接口时，应当遵循以下策略和限制。

- 以下限制应用于 Cisco IOS 12.2(18)SXE 及更早的版本。

① 子接口只支持 MPLS。

② 不能配置 ISL 封装。

- 当 VLAN ID 是 IEEE 802.1q 本地 VLAN（Native VLAN）时，总是使用 native 关键字。不能在没有 native 关键字的 802.1q 中继的本地 VLAN 配置封装。
- 由于 VLAN ID 被全局应用于交换机，因此，可以在子接口或者作为三层 VLAN 的接口上使用内部 VLAN。

① 不能在子接口或三层 VLAN 接口上配置内部 VLAN。

② 不能在三层 VLAN 接口上配置子接口 VLAN。

③ 不能在子接口上配置 VLAN 作为三层 VLAN 接口使用。

提·示 不能在另一个接口或子接口上配置一个用于当前接口或子接口的 VLAN。

在 VTP 透明模式中，不能为子接口配置任意标准范围或扩展范围 VLAN ID。因为 1～1005 是 VTP 域中的全局 VLAN ID，不能在 VTP 域中的其他网络设备上定义，只能为处于 VTP 客户端或服务器模式的子接口使用扩展范围的 VLAN ID。在 VTP 客户端或服务器模式中，标准范围 VLAN 从子接口中被排除。

提·示 如果在子接口配置了标准范围的 VLAN，不能从透明模式中改变 VTP 域模式。

■ **配置命令**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置的接口，进入子接口配置模式。Type 可以是 ethernet、fastethernet、gigabitethernet、tengigabitethernet 或 ge-wan。Subinterface 的可取值范围为 1～4 294 967 293。

`Switch(config)#` interface {{*type slot/port.subinterface*} | {port-channel *port_channel _number.subinterface*}}

③ 为子接口配置 802.1q 封装。vlan_ID 指定封装的 VLAN，native 用于指定本地 VLAN。

```
Switch(config-subif)# encapsulation dot1q vlan_ID [native]
```

④ 返回特权配置模式。

```
Switch(config-subif)# end
```

⑤ 校验配置。

```
Switch#show interface interface_id.subinterface
```

6.4.5 配置单播路由

VLAN 作为一种虚拟的局域网，不同 VLAN 之间是不能直接通信的，彼此之间的数据传输必须借助路由器或内置路由功能的三层交换机。因此，在网络中必须恰当地配置一个或多个路由设备（三层交换机或路由器），才能将数据转发至目的 VLAN，实现整个网络的通信。

1. 交换机支持的路由与协议类型

路由器和三层交换机能够以三种不同的方式路由数据包。

- 默认路由（Default Routeing）
- 预先订制的静态路由（Static Route）
- 使用路由协议动态计算的路由（Dynamically Route）

默认路由将把所有未知目的的通信路由至默认出口或目的接口。

静态单播路由由预先确定的端口以单一进出路径转发包。静态路由是安全的，并且使用较小的带宽，但是，不能自动响应网络的改变，如链路失败，因此，可能导致不能到达目的。由于静态路由需要全部由管理员手工进行维护，因此，对于成长迅速或变化较快的网络而言，选择使用静态路由将面临着巨大的任务量。

动态路由使用路由协议，能够动态计算最佳路由并转发通信。有两种类型的动态路由协议：

- 路由器使用距离矢量（Distancd-vector）维护路由表，并且周期性地向其邻居发送这些路由表。距离矢量协议使用一个或一系列测量计算最佳路由。这类协议容易被配置和使用。
- 路由器使用链路状态协议（Link-state Protocol），基于在路由器之间交换链路状态公告（Link-state Advertisement，LSA）维护一个复杂的网络拓扑数据库。链路状态协议能够快速响应拓扑的改变，但是，也需要更大的带宽和更多资源。

交换机支持的距离矢量协议为使用单一距离开销确定最佳路径的 RIP（Routing Information Protocol，路由消息协议），添加路径矢量结构的 BGP（Border Gateway Protocol，边界网关协议）。交换机也支持 OSPF（Open Shortest Path First，开放最短路径优先）链路状态协议，和在 IGRP（Interior Gateway Routing Protocol，内部网关路由协议）中添加了一些链路状态路由功能的 EIGRP（Enhanced IGRP，增强内部网关路由协议）。

> **提·示** 交换机或交换机堆叠能够支持的路由协议取决于在交换机或堆叠主交换机上运行的 Cisco IOS 软件版本。如果运行的是 IP Base 功能版本，将只支持默认路由、静态路由和 RIP 动态路由。其他所有路由协议，则需要 IP Services 功能版本才能支持。

2. 路由配置步骤

默认情况下，交换机的 IP 路由处于被禁用状态，因此，必须启用路由配置。路由配置通常都需要以下几个重要步骤。

① 支持 VLAN 接口，在交换机或交换机堆叠上创建并配置 VLAN，并将二层接口指定为 VLAN 成员。

② 配置三层接口。

③ 在交换机上启用 IP 路由。

④ 为三层接口指定 IP 地址。

⑤ 在交换机上启用选择的路由协议。

⑥ 配置路由协议参数（可选）。

用于实现路由转发的接口必须是三层接口。三层接口包括以下三种类型。

- 路由接口。使用 no switchport 接口配置命令，将物理端口配置为三层接口。
- 交换虚拟接口（SVI）。使用 interface vlan *vlan_id* 全局配置命令创建的 VLAN 接口，默认状态下是三层接口。
- 三层模式的 EtherChannel Port-Channel 接口。使用 interface port-channel *port-channel-number* 全局配置命令创建的 Port-Channel 逻辑接口，将以太网接口绑定至 Channel 组。

用于路由的三层接口，必须都配置有 IP 地址信息。

> **提·示** 在三层交换机中，可以为每个路由接口和 SVI 接口指定一个 IP 地址。虽然 Cisco IOS 并没有限制三层交换机路由接口和 SVI 接口的数量，但是，鉴于硬件的限制，当三层接口的数量太多时，将会大幅提高 CPU 的利用率。因此，即使是 Catalyst 6500 系列交换机，也推荐配置不超过 2000 个 VLAN 接口。Catalyst 3850 则建议配置不超过 128 个路由端口和 SVI。另外，使用 sdm prefer routing 全局配置命令，可以优化路由的系统内存。

3. 默认 IP 地址配置

三层接口的默认 IP 地址配置如表 6-10 所示。

表 6-10 三层接口的默认 IP 地址配置

特　　性	默认配置
IP 地址	未定义
ARP	ARP 缓存中没有永久性条目 封装：标准以太网 ARP 超时：14 400 s（4h）

（续表）

特　　性	默认配置
IP 广播地址	255.255.255.255
IP 无类路由	启用
IP 默认网关	禁用
IP 定向广播	禁用（所有 IP 定向广播被丢弃）
IP 域	域列表：没有域名定义 域查找：启用 域名：启用
IP 转发协议	如果定义了 Helper 地址或配置了 UDP 泛洪，默认端口上的 UDP 转发将被启用 Any-local-broadcast：禁用 STP：禁用 Turbo-flood：禁用
IP Helper 地址	禁用
IP 主机	禁用
IRDP（ICMP 路由发现协议）	禁用
IP 代理 ARP	启用
IP 路由	禁用
IP 子网零	禁用

4. 使用子网零

划分为 0 的子网地址原则上是不允许的，因为这可能会导致一个网络和一个子网拥有相同 IP 地址的问题。例如，假设网络 10.20.0.0 是一个子网掩码为 255.255.255.0 的子网，而子网零（Subnet Zero）也将被写为 10.20.0.0，也就是说，与网络地址完全相同。

如果确实需要这些子网空间所提供的 IP 地址，那么，不妨启用子网零，以使用所有的子网（如 10.20.255.0），尽管这并不是推荐的。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 在接口地址和路由更新中使用子网零。

```
Switch(config)# ip subnet-zero
```

③ 退出配置模式。

```
Switch(config)# end
```

④ 校验配置。

```
Switch# show running-config
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

使用 no ip subnet-zreo 全局配置命令，可以恢复系统默认值，并禁用子网零。

5. 启用 IP 无类路由

无类路由（Classless Routing）可以在每个网络段中使用不相同的子网掩码，RIPv2、EIGRP、

OSPF 和 BGP 等路由选择协议，在路由更新过程中，将网络掩码与路径一起广播出去。也就是说，无类路由（如 RIP、IGRP 等）在通告时携带网络掩码，而有类路由（Classful Routing）在通告时不携带网络掩码。

使用有类路由时，路由器首先匹配主网络号，如果主网络号存在，就继续匹配子网号，且不考虑缺省路由。如果子网无法匹配，丢弃数据包（在分类路由下，路由器认为知道所有主网络下的全部子网），并使用 ICMP 返回一个不可达回应。如果主网络号不存在，则使用缺省路由（以存在缺省路由为前提）。使用无类路由时，如果没有找到最具体的匹配，即使用缺省路由。ip classless 命令的作用主要是改变有类路由协议的查找路由表的行为，路由器将进行最长最精确匹配或使用默认路由进行匹配。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 启用 IP 无类路由。

```
Switch(config)# ip classless
```

③ 退出配置模式。

```
Switch(config)# end
```

④ 校验配置。

```
Switch# show running-config
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

使用 **no ip classless** 使用命令可以禁用 IP 无类路由。

6. 启用 IP 单播路由

默认状态下，Cisco Catalyst 3xxx 系列交换机的 IP 路由是被禁用的，Catalyst 4xxx/6xxx 系列交换机的 IP 路由是被启用的。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 启用 IP 单播路由。

```
Switch(config)# ip routing
```

③ 指定 IP 路由协议。当采用动态路由协议时，还需要设置其他参数。详细配置内容参见“第 13 章 使用 CLI 配置路由器”。IP Base 版本只支持 RIP 动态路由协议。

```
Switch(config)# router ip_routing_protocol
```

④ 退出配置模式。

```
Switch(config)# end
```

⑤ 校验配置。

```
Switch# show running-config
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

使用 no ip subnet-zreo 全局配置命令，可以恢复系统默认值，并禁用子网零。

6.4.6 配置缺省网关和默认路由

1. 配置缺省网关

当路由器上的 ip routing 无效时，使用 ip default-gateway 命令配置缺省网关，用于 RXBoot 模式（no ip routing）下安装 IOS 等，或者关闭 ip routing 让路由器当主机用。

默认网关的配置过程如下：

① 进入全局配置模式。

```
Switch# configure terminal
```

② 设置缺省网关（路由）。

```
Switch(config)# ip default-gateway ip-address
```

③ 退出配置模式。

```
Switch(config)# end
```

① 校验配置。

```
Switch# show running-config
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

2. 配置默认路由

默认路由告诉路由器，当数据包的目的地址不与路由表中的任何路由相匹配时，将其发送至何处。如果没有配置默认路由，那么，当收到在路由表中没有目的地址的数据包时，路由器将会丢弃这个数据包。而一旦设置了默认路由，路由器将根据默认路由的指示发送该数据包。

默认路由主要应用于两种情形：

- 局域网中的路由器只有一条可能的物理路径将数据包发送至网络的其他部分。
- 从局域网到 Internet 只有一个连接。

可见，对于两层结构的局域网而言，与上述指定的两种情形完全符合。

ip default-network 和 ip route 0.0.0.0 0.0.0.0 两者都用于 ip routing 有效的路由器上，区别主要在于路由协议是否传播这条路由信息。例如，IGRP 无法识别 0.0.0.0，因此传播默认路由时必须用 ip default-network。

当用 ip default-network 指令设定多条默认路由时，administrative distance 最短的成为最终

的默认路由；如果有多条路由 distance 值相等，那么在路由表（show ip route）中靠上的成为默认路由。

同时，使用 ip default-network 和 ip route 0.0.0.0 0.0.0.0 设定默认路由时，如果 ip default-network 设定的网络是直连（静态且已知），那么它就成为默认路由；如果 ip default-network 指定的网络是由交换路由信息得来的，则 ip route 0.0.0.0 0.0.0.0 指定的表项成为默认路由。

最后，如果使用多条 ip route 0.0.0.0 0.0.0.0 指令，则流量会自动在多条链路上负载均衡。

默认路由的配置命令非常简单，即将所有未知访问全部路由至指定的三层逻辑接口或三层物理接口。

① 进入全局配置模式。

```
Switch# configure terminal
```

②（可选）启用 IP 路由。如果尚未启用 IP 路由，则必须启用 IP 路由。

```
Switch(config)# ip routing
```

③ 将所有未知访问路由至指定的三层逻辑接口。

```
Switch(config)# ip route 0.0.0.0 0.0.0.0 ip-address
```

或者，将所有未知访问路由至指定的三层物理接口。

```
Switch(config)# ip route 0.0.0.0 0.0.0.0 interface_id
```

或者，将所有未知访问路由至指定网络。

```
Switch(config)# ip default-network network-number
```

对于 IGRP/EIGRP 还必须宣告其所在网络。

```
Switch(config)# network network-number
```

④ 返回至特权配置模式。

```
Switch(config-if)# end
```

⑤ 查看并校验配置。

```
Switch# show running-config
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

6.4.7 配置动态路由

在规模较大的三层结构网络中，由于汇聚层交换机大多采用路由方式实现与核心层交换机的连接，同时，核心层交换机又往往采用双核心架构，因此，使用动态路由方式实现核心层交换机与汇聚层交换机之间的通信应当是首要选择。

Cataly 4500/4900/6500 系列交换机支持 RIP、OSPF、EIGRP、BGP 和 IS-IS 等动态路由协议。Catalyst 3560/3750/3850 系列交换机支持 RIP、OSPF、EIGRP 和 BGP 等动态路由协议。

如果网络中全部采用 Cisco 产品，那么，可以选择使用 RIP、OSPF 或 EIGRP 动态路由协

议实现骨干层彼此之间的三层互连。如果网络中既有 Cisco 产品，也有第三方产品，那么，将只能采用 RIP 或 OSPF 动态路由协议实现三层互连。

三层交换机动态路由协议的配置与路由器基本相同，故此处不复赘述。具体配置请参见“第 13 章使用 CLI 配置路由器”。

当然，在启用动态路由之前，应当将与三层汇聚层交换机相连接的端口设置为三层接口，并为其配置 IP 地址信息。

6.5 配置端口

交换机端口用于连接其他网络设备和计算机，或者说，交换机是依靠其端口才实现与其他设备的连接，从而构建局域网络的。端口速率、双工模式设置是否正确、端口之间的参数设置是否匹配，从根本上决定着设备之间能否正常进行通信。

6.5.1 配置二层接口

通常情况下，端口的传输速率和双工模式无需另行配置，可以采用系统默认值。但为了便于实现对端口的远程管理，应当为每个端口都键入描述文字。同时，为了降低端口配置的复杂性，可以将若干端口指定为端口组，从而将相关配置一次应用于该端口组内的所有端口。

1. 二层以太网接口默认配置

二层以太网接口默认配置如表 6-12 所示。

表 6-12 二层以太网接口默认配置

特　　性	默认配置
允许 VLAN 范围	1～4094
运行模式	二层或交换模式（switchport 命令）
默认 VLAN	VLAN 1（仅指二层接口）
本地 VLAN（IEEE 802.1q）	VLAN 1（仅指二层接口）
VLAN 中继	Switchport mode dynamic auto (支持 DTP，仅指二层接口)
端口启用状态	所有端口都被启用
端口描述	未定义
速率	自适应（10 Gbps 接口不支持）
双工模式	自适应（10 Gbps 接口不支持）
流量控制	设置为 receive: off
EtherChannel (PAgP)	在所有以太网端口禁用
端口阻塞（未知多播和单播传输）	禁用（未阻塞）
广播、多播和单播风暴控制	禁用（未阻塞）
保护端口	禁用
端口安全	禁用
PortFast	禁用
Auto-MDIX（自动翻转）	启用（需要交换机硬件支持。Catalyst 2950/3550/4000 等老型号交换机不支持）
PoE	启用（自动）
Keepalive 消息	SFP/GBIC 模块端口禁用，其他所有端口启用

> **提·示** 默认状态下，所有接口都被启用。100Base-TX 以太网接口自动协商（Autonegotiate）连接速率和双工模式。1000Base-T 以太网接口自动协商速率、双工模式和流量控制。1000 Mbps 以太网接口只协商流量控制。自动协商能够自动选择所能实现的最高速率。当接口的速率被明确指定时，那么，该接口默认将采用半双工模式，除非明确指定其采用全双工模式。

2. 配置复用端口

某些型号接入交换机（如 Catalyst 2960）的 Uplink 端口选择使用复用端口，以获得更多的连接灵活性。复用端口虽然支持两种媒体类型，即 SFP 和 RJ-45，但是同一复用端口的两种媒体并不能同时使用，而只能使用其中一种类型。默认情况下，交换机根据第一次连接动态选择接口类型。当然，也可以使用 media-type 接口配置命令手动选择 RJ-45 连接器或 SFP 模块连接器。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲选择媒体类型的 Uplink 复用接口或接口范围。

```
Switch（config）# interface interface_id
```

或者

```
Switch（config）# interface range interface-range
```

③ 在复用 Uplink 端口选择接口和媒体类型。关键字 auto-select，允许交换机自动动态选择媒体类型。当连接完成后，交换机禁用另一种媒体类型，直至活动连接宕掉（Down）。当活动连接宕掉时，交换机启用两种类型直至其中之一连接恢复。在 auto-select 模式中，交换机将两种类型均配置为速度和双工模式自适应。关键字 rj45 使交换机禁用 SFP 模块接口。即使将一个 SFP 模块连接到该接口，在 RJ-45 端口宕掉或没有连接之前，该连接仍然不可用。在该模式下，复用端口就像一个 1000Base-T 接口，可以手工配置该接口的速率和双工模式。关键字 sfp 使交换机禁用 RJ-45 接口。尽管可以连接一条电缆至 RJ-45 端口，然而，在 SFP 模块宕掉或 SFP 模块没有插入之前，该连接仍然不可用。

```
Switch（config-if）# media-type {auto-select | rj45 | sfp}
```

④ 返回至特权配置模式。

```
Switch（config-if）#end
```

⑤ 查看并校验配置。

```
Switch# show interfaces interface_id transceiver properties
```

⑥ 保存修改的配置。

```
Switch# copy running-config startup-config
```

3. 端口基本配置

端口基本配置的内容包括速率、全双工模式和端口描述。

■ **配置策略**

在配置接口速度和双工模式时，应当遵循以下配置策略。

- 快速以太网端口（100 Mbps）支持所有速率和双工模式选项。
- 千兆位以太网（1 000 Mbps）端口支持所有速率选项和所有双工选项（自动、半双工和全双工）。不过，在 1000 Mbps 速率上运行的千兆位以太网端口不支持半双工模式。
- 如果连接的两端均支持自适应，强烈推荐采用默认的 auto 设置，使其自动协商，避免可能由于速率或双工模式配置错误导致的链路失败。
- 如果连接中只有一端支持自适应，应当在两个接口都配置双工和相同速率，而不要在支持自适应的一端使用 auto 设置。
- 配置 10 Gbps 以太网接口，不能手工配置速率和双工模式，也不支持 IP 电话的 Auto-QoS。
- 当 10 Gbps 模块端口被配置为 SPAN 或 RSPAN 目的端口时，链路速率会下降。
- 支持最多 2 个跨堆叠的 10 Gbps 模块创建 EtherChannel。

■ **配置过程**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置的端口，进入接口配置模式。

```
Switch(config)# interface interface_id
```

③ 设置接口速率。1000 和 auto 关键字只对 1000Base-T 端口有效；光纤 GBIC/SFP 模块端口只能工作于 1000 Mbps；Nonegotiate 关键字只对 GBIC/SFP 端口有效。

```
Switch(config-if)# speed [10 | 100 | 1000 | auto | nonegotiate]
```

④ 设置双工模式。1000 Mbps 端口和插槽只能工作于全双工模式；duplex 关键字对 GBIC/SFP 端口和 1000Base-T 端口无效。

```
Switch(config-if)# duplex [auto | full | half]
```

⑤ 在接口启用自动翻转（Auto-MDIX）。自动翻转支持所有的 100Base-TX 和 1000Base-T 接口，但是，不支持光纤 SFP 模块。在配置自动翻转前，应当将接口的速率和双工模式都设置为 auto。

```
Switch(config-if)# mdix auto
```

> **提·示** 启用自动翻转后，端口将根据对端所连接的设备自动选择和切换连接方式，因此，即使对端连接至交换机，也不必再使用交叉线。不过，只有新型交换机（如 Catalyst 2960/3560/3750）才支持该功能。

⑥ 为端口指定描述文字，可以直观地了解该端口所连接的设备（如 Connect to liuxh 或 Connect to xiaolf），从而便于进行配置和管理。最多允许 240 个字符。

```
Switch(config-if)# description string
```

⑦ 返回特权配置模式。

```
Switch(config-if)# end
```

⑧ 显示接口状态和文字描述。

```
Switch# show interfaces interface_id
Switch# show interfaces interface_id description
```

⑨ 保存配置。

```
Switch# copy running-config startup-config
```

4. 配置端口组

许多端口的配置都完全相同。分别配置一个个端口既太过繁琐，又容易出错。将若干端口定义成一个端口组后，只需设置该端口组，所包含的端口即可拥有相同的配置。

■ **指定端口范围**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置的端口范围，进入接口配置模式。

```
Switch(config)# interface range interface-range
```

③ 键入 CLI 命令，将对所有指定的端口生效。
④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 显示当前运行的配置。

```
Switch# show running-config
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

在指定端口范围时，注意以下几个方面的问题。

- 有效的端口范围

vlan *vlan_id*：VLAN ID 的取值范围为 1～1005（SI 版软件），或 1～4094（EI 版软件）。
fastethernet *slot*/{*first port*} - {*last port*}：*slot* 的值为 0。
gigabitethernet *slot*/{*first port*} - {*last port*}：*slot* 的值为 0。
port-channel *port-channel-number* - *port-channel-number*：port-channel-number 的取值范围为 1～6。

- 连字符

连续的端口号可以在起止端口号间使用连字符表示。不过，必须在连字符“-”的前后都添加一个空格。例如，fastethernet 0/1 - 5 是正确的，而 fastethernet 0/1-5 则是错误的。

- 端口类型

端口组内的所有端口都必须是相同类型的，或者全部为 Fast Ethernet 端口、Gigabit Ethernet 端口、TenGigabit Ethernet 端口、EtherChannel 端口，或者全部为 VLAN。

■ **定义端口组宏**

如果需要频繁地配置某个端口组，可以将该端口组设置为端口组宏，针对该宏所作的设置，将应用至每个端口。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为指定的若干端口定义端口组宏名称，并将其保存在 NVRAM 中。宏名称最大为 32 个字符。一个宏最多可以使用 5 个逗号，来指定端口范围，并且不需要在逗号之间加入空格。不过，每个端口组都必须由相同类型的端口组成。

```
Switch(config)# define interface-range macro_name interface-range
```

③ 使用宏名称选择被配置的端口组。保存的用于指定端口范围的宏称为宏名称。然后，即可使用 CLI 命令对这些端口进行配置，命令将对指定的所有端口生效。

```
Switch(config)# interface range macro macro_name
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 显示当前运行的配置。

```
Switch# show running-config
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

6. 宕掉并重启接口

当接口由于某种原因出错时，可以将端口宕掉重新启用一下，以恢复其可用性。当然，也可直接使用 no shutdown 接口配置命令启用已经宕掉的端口。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface_id
```

③ 宕掉（down）接口。

```
Switch(config-if)# shutdown
```

④ 重新启用端口。

```
Switch(config-if)# no shutdown
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 查看指定接口当前状态。

```
Switch# show interface interface_id
```

⑦ 保存配置。

```
Switch# copy running-config startup-config
```

6.5.2 配置 PortFast

Portfast 快速端口是 Cisco Catalyst 交换机的一个特有功能，能使交换机或中继端口跳过侦听学习状态而进入 STP 转发状态，在基于 IOS 交换机上，PortFast 只能用于连接到终端工作站的接入端口上。

> **注意** PortFast 通常只被应用于接入交换机。如果在其他网络设备（如交换机）连接上启用 PortFast，将可能在冗余链路上形成网络环，从而导致网络瘫痪。

1. PortFast 简介

为了避免网络中存在拓扑环，从而导致网络瘫痪，可网管交换机默认状态下都启用生成树协议。这样，即使网络中存在环路，也会只保留一条路径，而自动切断其他链路。所以，当交换机在加电启动时，各端口需依次进入监听、学习和转发（或阻塞）状态。在监听和学习状态中，不能进行信息的转发。

然而，当在那些直接连接至终端（普通客户端、网络服务器、网络打印机等）的交换机端口上使用 PortFast 时（如图 6-1 所示），Spanning-Tree PortFast 将使端口绕过监听和学习阶段，立即进入 Spanning-Tree 转发状态，避免了端口由监听和学习状态向转发状态过渡的等待。

当交换机检测到链路，端口就进入转发状态（插电缆后的 2 s）。如果端口检测到一个环路，同时又启用了 PortFast 功能，那么，它将进入阻塞状态。不过，PortFast 只在端口初始化的时候才生效。如果端口由于某种原因又被迫进入阻塞状态，随后又需要回到转发状态，仍然要经过正常的侦听。

> **提示** PortFast 仅仅让端口在网络环境变化的情况下直接进入转发状态，端口仍然运行 STP 协议，所以，如果检测到环路，端口仍将由转发状态变成阻塞状态。

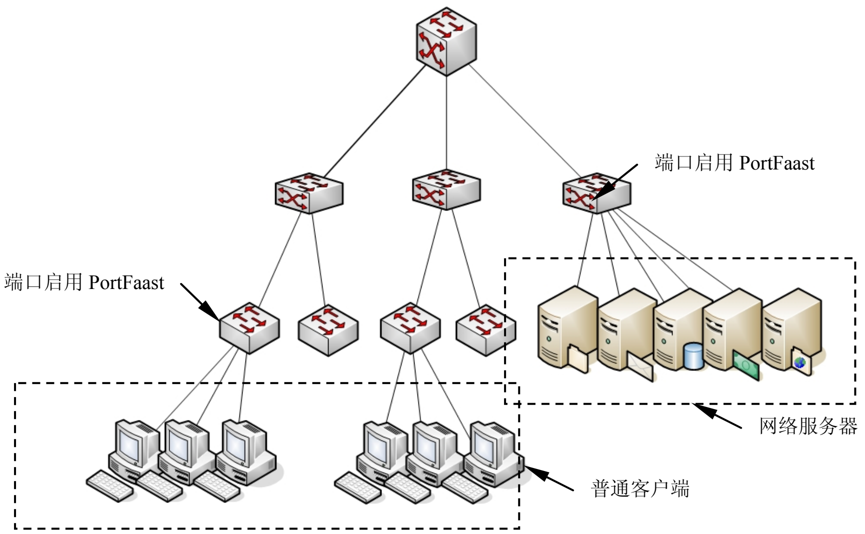


图 6-1　PortFast

2.　配置 PortFast

当交换机运行 PVST+、rapid PVST+或 MSTP 时，即可在接口应用 PortFast，以实现计算机和其他终端设备的快速接入。

① 进入配置模式。

```
Switch# configure terminal
```

② 选择欲配置的接口或接口范围。

```
Switch(config)# interface interface_id
```

或者

```
Switch(config)# interface range interface-range
```

③ 在直接连接至计算机的端口上启用 Port Fast。指定 trunk 关键字，可以在 Trunk 端口启用 Port Fast。默认状态下，所有端口都禁用 Port Fast。

```
Switch(config-if)# spanning-tree portfast [trunk ]
```

④ 返回特权配置模式。

```
Switch(config)# end
```

⑤ 校验配置。

```
Switch# show spanning-tree interface interface_id portfast
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

使用 spanning-tree portfast default 全局配置命令，可以在所有非 Trunk 端口上都启用 Port

Fast 功能。使用 spanning-tree portfast disable 接口配置命令，可以禁用 Port Fast 功能。

另外，也可以在指定的 VLAN 内禁用 spanning-tree，从而使所有端口立即进入转发状态。操作如下：

① 进入配置模式。

```
Switch# configure terminal
```

② 选择欲配置的接口。

```
Switch(config)# no spanning-tree vlan vlan_id
```

③ 保存配置。

```
Switch# copy running-config startup-config
```

注·意 Portfast 可以应用于所有单独的端口，也就是说，当某个端口启用 Portfast 时，不会影响到其他端口。而禁用 Spanning Tree，则将在整个 VLAN 中的所有端口上都禁用生成树，从而不能在整个 VLAN 中有任何冗余链接，否则将产生灾难性的后果。

6.5.3 配置 UplinkFast

STP 虽然确保了在拓扑变化的情况下没有环路产生，但是收敛速度太慢，对于一些实时或对带宽敏感的网络应用是不能接受的。STP 收敛速度慢的原因是收敛算法需要花时间确定一条可替代的链路，默认时间是 50 s，即 20 s（阻塞→侦听）+15 s（侦听→学习）+15 s（学习→转发）。解决的方法是一旦发现了线路宕掉，马上将阻塞的端口切换到转发，不必再经历侦听和学习阶段，这就是 UplinkFast。UplinkFast 切换时间可以在 2～4 s 范围内。UplinkFast 被设计应用于接入层交换机，使用两条上行链路连接到分布层，其中一条是活跃链路，而另一条则是冗余链路。

1. UplinkFast 简介

在分层网络环境中，交换机被划分为不同的组，即核心（或称骨干）交换机、汇聚（或称分布）交换机和访问（或称接入）交换机。图 6-2 所示为在复杂网络中，分布交换机和访问交换机都拥有冗余链接，并借助 STP 阻塞防止生成环路。

交换机失去连接，将开始使用备份路径，STP 将选择一个新的端口。当启用 UplinkFast 后，在交换机或连接失败后，可以在 STP 重新配置的过程，加快选择新根端口的速度。根端口将立即过度到转发状态，而不再像普通 STP 那样，需要经过侦听和学习状态。

当 STP 重新配置新的根端口时，其他接口以多播包泛洪网络，该接口上的每个地址都将被学习。可以通过设置 max-update-rate 参数［默认值为 150 PPS（包每秒）］限制多播传输。然而，如果键入 0，状态学习帧将不能生成，在连接失败后 STP 收敛将更慢。

UplinkFast 在直连链路失败后提供快速收敛，并且借助 Uplink（上行）组在冗余二层链路间实现负载分担。Uplink 组是一个二层接口，仅用于数据转发。具体来说，Uplink 组由根端

口（处于转发状态）和阻塞端口组成，自我循环端口除外。Uplink 组为失败的转发连接提供了一条备份路径。

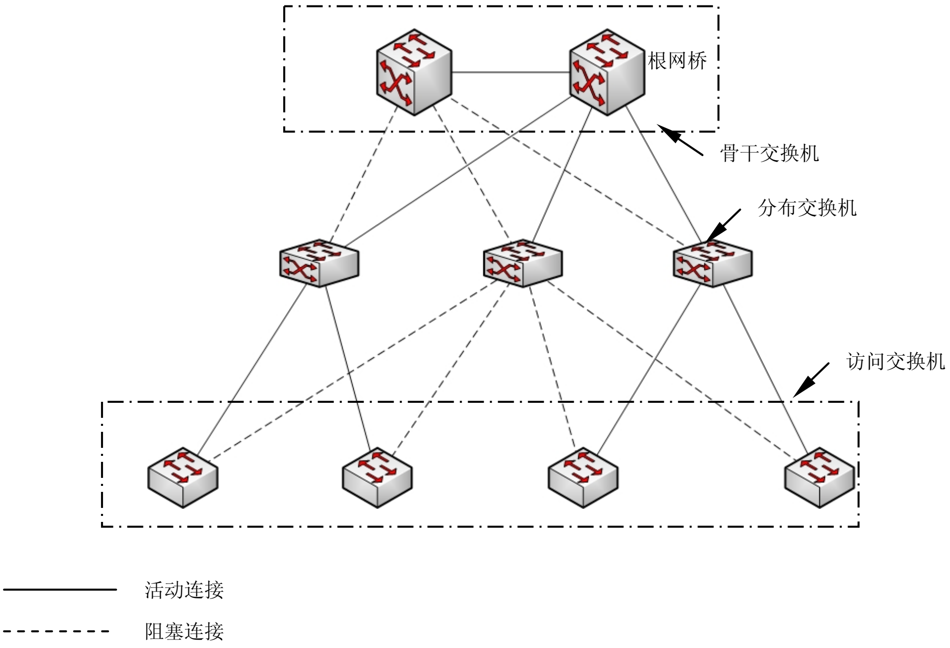


图 6-2　分层网络结构

图 6-3 所示为没有连接失败时的拓扑结构。根交换机 Switch A 借助链路 L1 直接连接到 Switch B，并通过链路 L2 直接连接到交换机 Switch C。交换机 Switch C 上直接连接 Switch B 的二层接口处于禁用状态。

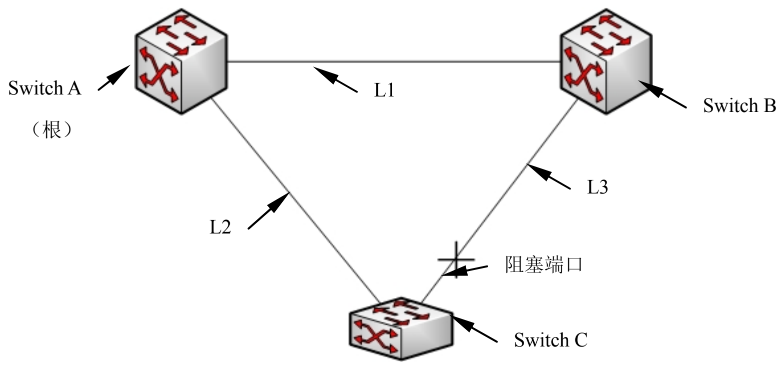


图 6-3　没有连接失败时的拓扑结构

当 Switch C 察觉到连接根端口的活跃链路 L2（直连连接）失败后，UplinkFast 将解除 Switch C 交换机的阻塞端口，并直接转换至转发状态（如图 6-4 所示），而忽略掉侦听、学习状态。状态改变完成通常只需 1～5 s，因此，大致可节约 30 s 的延迟。主要用于接入层，一条是上行链路，一条是冗余链路的拓扑中。

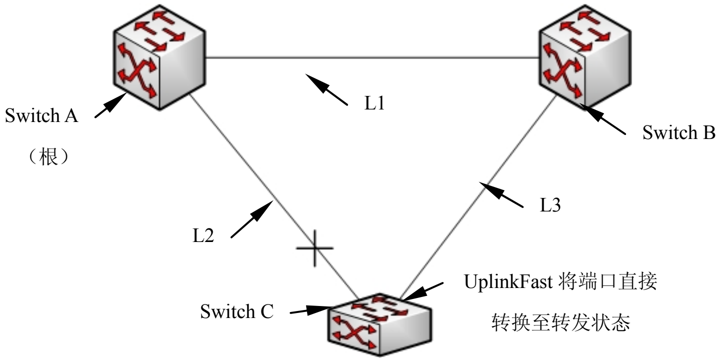


图 6-4　L2 连接失败

一个 UplinkFast 组由根端口和除自环端口之外的一组阻断端口组成，上行链路使交换机上的一个阻断端口几乎立刻进行转发。很重要的一点就是，UplinkFast 只能配置在接入层交换机上，因为从根端口到其非指定备份端口的快速转发只能在生成树拓扑结构的根端口上完成。

可见，UplinkFast 激活快速重新配置需要以下几个条件。

- 在交换机上必须启动了 UplinkFast 功能。
- 至少有一个处于阻塞的端口（即有冗余链路）。
- 链路失效必须发生在根端口上。

启用 UplinkFast 后，所有 VLAN 的交换机优先级都将被设置为 49152。如果将路径开销值修改为小于 3000，并启用 UplinkFast 或者 UplinkFast 已经被启用，所有接口和 VLAN Trunk 的路径开销都将增加 3000（如果将路径开销设置为 3000 或以上，将不会被修改）。修改交换机优先级和路径开销将减少交换机改变为根交换机的机会。

2.　启用 UplinkFast

UplinkFast 默认是全局禁用的，因此，若欲使用 UplinkFast 功能，就必须手工启用。另外，UplinkFast 不能在配置有交换机优先级的 VLAN 中启用，因此，必须先使用 no spanning-tree vlan *vlan-id* priority 全局配置命令将交换机的优先级恢复至默认值。

> **注意：** 启用 UplinkFast 将影响所有的 VLAN。也就是说，不能仅在某个 VLAN 中配置 UplinkFast。另外，虽然能够为 rapid PVST+或 MSTP 配置 UplinkFast 特性，但是，其他特性在改变为 PVST+前将禁用。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 启用 UplinkFast。（可选）*pkts-per-second* 取值范围为 0～32 000 PPS，默认为 150。

```
Switch(config)# spanning-tree uplinkfast [max-update-rate pkts-per-second]
```

③ 返回特权配置模式。

```
Switch(config-if)# end
```

④ 校验当前设置。

```
Switch# show spanning-tree summary
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

当 UplinkFast 被禁用，所有 VLAN 的交换机优先级和所有接口的路径开销都将被设置为其默认值。

若欲将更新包速率恢复至默认值，可使用 no spanning-tree uplinkfast *max-update-rate* 全局配置命令；若欲禁用 UplinkFast，可使用 no spanning-tree uplinkfast 命令。

6.6 基于端口的传输控制

借助对端口传输控制的配置，既可以有效杜绝广播风暴对整个网络的冲击，从而保证网络的正常通信。同时，又可以拒绝未被授权的计算机接入网络，或者限制某个端口接入计算机的数量，从而保证网络的接入安全，避免网络被个别用户滥用。

6.6.1 风暴控制

当端口接收到大量的广播、单播或多播包时，就会发生广播风暴。转发这些包将导致网络速度变慢或超时。借助于对端口的广播风暴控制，可以有效地避免因硬件损坏或链路故障而导致的网络瘫痪。默认状态下，广播、多播和单播风暴控制被禁用。

1. 启用风暴控制

① 进入配置模式。

```
Switch# config terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

③ 配置广播、多播或单播风暴控制。默认状态下，风暴控制被禁用。

- level，指定阻塞端口的带宽上限值。当广播、多播或单播传输占到宽带的很大比例（百分比）时，端口将阻塞传输。取值范围为 0.00～100.00。如果将值设置为 100%，将不限制任何传输；如果将值设置为 0%，那么该端口的所有广播、多播和单播都将被阻塞。
- level-low，指定启用端口的带宽下限值。该值应当小于或等于下限值，当广播、多播或单播传输占用带宽的比例低于该值时，端口恢复转发传输。取值范围为 0.00～100.00。
- bps，指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特（bps）时，端口将阻塞传输。取值范围为 0.0～10 000 000 000.0。
- bps-low，指定端口启用的传输速率下限值。该值应当小于或等于下限值，当广播、多播或单播传输低于每秒若干比特（bps）时，端口将恢复传输。取值范围为 0.0～10 000 000 000.0。如果数值较大，也可以使用 K、M 或 G 等单位表示。

- pps，指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干包（pps）时，端口将阻塞传输。取值范围为 0.0～10000000000.0。
- pps-low，指定端口启用的传输速率下限值。该值应当小于或等于下限值，当广播、多播或单播转发速率低于每秒若干包（pps）时，端口将恢复传输。取值范围为 0.0～10000000000.0。如果数值较大，也可以使用 K、M 或 G 等单位表示。

```
Switch(config-if)# storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}
```

④ 指定风暴发生时如何处理。默认状态下，将过滤外出的传输，并不发送 SNMP 陷阱。选择“shutdown”关键字，在风暴期间将禁用端口；选择“trap”关键字，当风暴发生时，产生一个 SNMP 陷阱，向网络管理软件发出警报。

```
Switch(config-if)# storm-control action {shutdown | trap}
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 显示并校验该接口当前的配置。

```
Switch# show storm-control [interface] [{broadcast | history | multicast | unicast}]
```

⑦ 保存风暴控制配置。

```
Switch# copy running-config startup-config
```

2. 禁用风暴控制

① 进入配置模式。

```
Switch# config terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

③ 禁用端口风暴控制。

```
Switch(config-if)# no storm-control {broadcast | multicast | unicast}
```

④ 禁用指定的风暴控制动作。

```
Switch(config-if)# no storm-control action {shutdown | trap}
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 显示并校验该接口当前的配置。

```
Switch# show storm-control [interface] [{broadcast | multicast | unicast}]
```

⑦ 保存配置。

```
Switch# copy running-config startup-config
```

6.6.2 端口流控制

流控制只适用于1000Base-T、1000Base-SX和GBIC端口。在千兆位端口启用流控制后，可以在拥塞期间暂停其他终端的连接。当端口处于拥塞状态，无法接收到数据流时，将通知其他端口暂停发送，直到恢复正常状态。当本地设备发现任何终端发生拥塞时，将发送一个暂停帧，以通知其连接伙伴或远端拥塞设备。收到暂停帧后，远程设备将停止发送任何数据包，以防止在拥塞期内丢失任何数据包。

> **提·示** 当在交换机中配置有QoS（Quality of Service）时，不要再配置IEEE 802.3x流控制。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 选择欲配置的端口，进入接口配置模式。

```
Switch(config)# interface interface-id
```

③ 设置端口的流控制。

```
Switch(config-if)# flowcontrol {receive | send} {on | off | desired}
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 显示接口状态。

```
Switch# show interfaces interface-id
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

6.6.3 端口带宽限制

网络传输速率变慢的主要原因往往是某些用户对网络的滥用。当使用MRTG等流量监控软件检测到流量来源于某个端口时，可以在核心层交换机、汇聚层交换机，甚至接入层交换机上，对相应的端口作必要的处理，限制其传输带宽，从而限制每个用户所允许的最大流量，以便使其他网络用户能够恢复正常的网络应用服务。

① 进入配置模式。

```
Switch# config terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

③ 配置端口带宽控制。其中，input/output 表明在输入和输出方向应用该带宽限制，通常情况下，应当进行双向限制。access-group *acl-index* 用于定义使用该带宽限制的访问列表。*bps* 用于定义限制带宽，以 bps 为单位，并采用 8 Kbps 的增量。burst-normal 用于定义所允许的普通突发速率，burst-max 用于定义所允许的最大突发速率。**conform-action** conform-action 用于指定在规定最大带宽时所执行的操作，通常为“transmit”即允许发送。**exceed-action** exceed-action 则用于指定在规定最大带宽时所执行的操作，通常为“drop”即丢弃。

```
Switch(config-if)# rate-limit {input | output} [access-group acl-index] bps burst-normal burst-max conform-action conform-action exceed-action exceed-action
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 显示并校验该接口当前的配置。

```
Switch# show interface interface-id
```

⑥ 保存带宽限制配置。

```
Switch# copy running-config startup-config
```

例如，若欲限制 GigabitEthernet4/4 带宽为 128 Kbps，当连接的普通突发速率、最大突发在 0～8 KBps（即 64 Kbps）、0～9 KBytes（即 72 Kbps）范围内时，所执行的操作是“transmit”（传输即发送）。当超出该范围时，则相应的操作就是“drop”。其中，128 000 用于限制最大带宽，8000 和 9000 则用于限制突发连接，保证不因个别用户的大量传输而使整个链路性能大幅度下降。限制输入和输出速率后，该端口配置如下：

```
interface GigabitEthernet4/4
 no switchport
 description tushuguan
 ip address 211.82.220.9 255.255.255.248
 ip access-group 120 in
 ip access-group 120 out
 rate-limit output access-group 102 128000 8000 9000 conform-action transmit exceed-action drop
 rate-limit input access-group 102 128000 8000 9000 conform-action transmit exceed-action drop
!
```

IP 访问列表只需设置应用带宽限制的 IP 地址范围（192.168.0.0～192.168.255.255）即可，内容如下。

```
access-list 102 permit ip 192.168.0.0 0.0.255.255 any
```

注·意 在启用宽带限制之前，必须先在全局模式下执行“ip cef”命令，启用交换机的快速转发技术。

6.6.4 保护端口

保护端口可以确保同一交换机上的端口之间不进行通信。保护端口不向其他保护端口转发任何传输，包括单播、多播和广播包。传输不能在第二层保护端口间进行，所有保护端口间的传输都必须通过第三层设备转发。保护端口与非保护端口间的传输不受任何影响。

① 进入配置模式。

```
Switch# config terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

③ 将接口配置为保护端口。

```
Switch(config-if)# switchport protected
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

⑥ 保存配置。

```
Switch# copy running-config startup-config
```

若欲禁用保护端口，可以使用“no switchport protected”接口配置命令。

6.6.5 端口阻塞

默认状态下，未知目的 MAC 地址的泛洪包被允许从端口向外传输。如果未知的单播和多播通信被转发到保护端口，将导致安全问题。可以采用阻塞端口的方式，防止未知的单播和多播通信被在端口间转发。

① 进入配置模式。

```
Switch# config terminal
```

② 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

③ 禁止未知多播从该端口向外传输。

```
Switch(config-if)# switchport block multicast
```

④ 禁止未知单播从该端口向外传输。

```
Switch(config-if)# switchport block unicast
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

⑦ 保存配置。

```
Switch# copy running-config startup-config
```

6.6.6 端口安全

借助安全端口，可以只允许指定的 MAC 地址或指定数量的 MAC 地址访问某个端口，从而避免未经授权的计算机接入网络，或限制某个端口所连接的计算机数量，从而确保网络接入的安全。

当配置端口安全时，应当注意以下问题。

- 安全端口不能是 Trunk 端口。
- 安全端口不能是 Switch Port Analyzer（SPAN）的目的端口。
- 安全端口不能是属于 EtherChannel 的端口。
- 安全端口不能是 private-VLAN 端口。

1. 配置安全端口

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置端口安全的接口。

```
Switch(config)# interface interface_id
```

③ 将接口设置为访问模式。

```
Switch(config-if)# switchport mode access
```

④ 在接口启用端口安全。

```
Switch(config-if)# switchport port-security
```

⑤（可选）在接口设置安全 MAC 地址的最大数量，以限制该端口所连接的计算机数量。取值范围为 1～3072，默认值是 1。

```
Switch(config-if)# switchport port-security maximum value
```

⑥（可选）设置违例发生后的处理模式。当安全违例事件发生时，将端口置于 restrict 或 shutdown 模式。选择 restrict 模式，当非法 MAC 地址或太多 MAC 连接至该接口时，将丢弃数据包，并向网管计算机发送 SNMP 陷阱通知。选择 shutdown 模式时，发生安全错误的端口将被置于 error-disable 状态，除非网络管理员使用“no shutdown”命令手工激活，否则该端口失效。

```
Switch(config-if)# switchport port-security violation {restrict | shutdown}
```

⑦ 设置坏包速率限制。

```
Switch(config-if)# switchport port-security limit rate invalid-source-mac
```

⑧ （可选）为该接口指定安全 MAC 地址。也可以使用该命令指定最大安全 MAC 地址数。如果指定的 MAC 地址数量少于安全地址的最大数量，动态学习的 MAC 地址将被保留。

```
Switch(config-if)# switchport port-security mac-address mac_address
```

⑨ 在端口启动 sticky learning。

```
Switch(config-if)# switchport port-security mac-address sticky
```

⑩ 返回特权 Exec 模式。

```
Switch(config-if)# end
```

⑪ 查看并校验配置。

```
Switch# show port-security address interface interface_id
Switch# show port-security address
```

⑫ 保存当前配置。

```
Switch# copy running-config startup-config
```

注·意 使用 no switchport port-security mac-address *mac_address* 命令，可以从地址表中删除 MAC 地址。

2. 设置端口安全老化

当为端口指定最大 MAC 地址数时，为了保障该端口能够得以充分利用，可以采用设置端口安全老化时间和模式的方式，使系统能够自动删除长时间未连接的 MAC 地址，从而不必手工删除，减少网络维护的工作量。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置端口安全老化的接口。

```
Switch(config)# interface interface_id
```

③ 为安全端口设置老化时间和老化类型。老化时间的取值范围为 0～1 440 min。采用 absolute 模式时，一旦到达指定的老化时间，即将其从安全地址列表中移除。采用 inactivity 时，即使到达指定的老化时间，如果没有其他通信数据，那么，MAC 地址仍然被保留在安全地址列表中。

```
Switch(config-if)# switchport port-security [ aging time aging_time | type {absolute|inactivity} ]
```

④ 返回特权 Exec 模式。

```
Switch(config-if)# end
```

⑤ 查看并校验配置。

```
Switch# show port security [interface interface_id] [address]
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

6.7 配置 ACL

访问控制列表（Access Control List，ACL）是 Cisco IOS 提供的一种访问控制技术，被广泛应用于路由器和三层交换机。借助 ACL，可以有效地控制用户对网络和 Internet 的访问，从而最大限度地保障网络安全，并使得企业网络不被滥用。

6.7.1 访问列表概述

ACL 使用包过滤技术，在路由器上读取第三层及第四层包头中的信息。如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。不过，由于 ACL 是通过使用包过滤技术来实现的，过滤的依据又仅仅只是第三层和第四层包头中的部分信息，这种技术具有一些固有的局限性。如无法识别到具体的人，无法识别到应用内部的权限类别等。因此，要达到“端到端”的权限控制目的，需要和系统级及应用级的访问权限控制结合使用。

1. 交换机支持的访问列表

交换机支持 IP 访问列表和 Ethernet（MAC）访问列表。

- IP 访问列表。过滤 IP 通信，包括 TCP、UDP（User Datagram Protocol，用户数据报协议）、IGMP（Internet Group Management Protocol，因特网组管理协议）和 ICMP（Internet Control Message Protocol，因特网控制消息协议）。
- Ethernet 访问列表。过滤非 IP 通信。

交换机支持三种访问列表的应用过滤传输。

- 端口访问列表。也称 MAC 访问列表。对进入二层接口的通信实施访问控制。交换机不支持外出访问的访问列表。在二层接口可以应用 IP 访问列表和端口访问列表。
- 路由访问列表。对 VLAN 之间以及三层接口之间的通信实施访问控制，并且可以控制进、出双向通信。
- VLAN 映射。也称 VLAN 访问列表，对所有包实现访问控制。在同一 VLAN 的设备之间，可以采用 VLAN 映射实施访问控制。VLAN 映射的配置与访问控制没有访方向，即基于 IP 地址和 MAC 地址。

可以在同一交换机上实施端口访问列表、路由访问列表和 VLAN 映射。不过，端口访问列表优先于路由访问列表和 VLAN 映射。

2. 访问列表的类型

Cisco 支持三种类型的访问列表，即标准 IP 访问控制列表、扩展 IP 访问控制列表和命名访问控制列表。

- 标准 IP 访问控制列表

标准 IP 访问列表只允许过滤源地址，且功能十分有限。当我们要想阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用标准访问控制列表来实现这一目标。标准访问控制列表检查路由的数据包的源地址，从而允许或拒绝基于网络、子网或主机的 IP 地址的所有通信流量通过路由器的出口。

- 扩展 IP 访问控制列表

扩展 IP 访问列表允许过滤源地址、目的地址和上层应用数据。因此，可以适应各种复杂的网络应用。扩展访问控制列表既检查数据包的源地址，也检查数据包的目的地址，还检查数据包的特定协议类型、端口号等。扩展访问控制列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其他协议的流量通过。

- 命名访问控制列表

在标准与扩展 IP 访问控制列表中均要使用表号，而在命名访问控制列表中使用一个字母或数字组合的字符串来代替前面所使用的数字。使用命名访问控制列表可以用来删除某一条特定的控制条目，这样可以在使用过程中方便地进行修改。

3. 配置访问列表应当注意的问题

在设置访问列表时，应当遵循最小特权原则，即只给受控对象完成任务所必须的最小的权限，从而最大限度地保障网络传输安全。所谓最小特权（Least Privilege），是指在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权。最小特权原则，则是指应限定网络中每个主体所必须的最小特权，确保可能因事故、错误、网络部件的篡改等原因造成的损失最小。最小特权原则一方面给予主体必不可少的特权，保证所有的主体都能在所赋予的权限内完成自己的任务或操作；另一方面，只给予主体必不可少的特权，从而限制每个主体所能进行的操作，以确保企业网络安全。

- 自上而下的处理过程

访问列表包含一个访问控制条目（Access Control Entry，ACE）规则列表。每个 ACE 都指定“permit”（允许）或“deny”（拒绝），以及应用条件。访问列表包会逐个条目顺序匹配 ACE。访问列表表项的检测按自上而下的顺序进行，并且从第一个表项开始。这意味着必须特别谨慎地考虑访问列表中语句的顺序。

- 添加表项

新增加的表项被追加到访问列表末尾，这就意味着不能改变已有的访问列表的功能。如果要改变，就必须创建一个新的访问列表，并删除已经存在的访问列表，并且将新的访问列表应用于接口上。

- 标准 IP 访问列表过滤

标准 IP 访问列表只限于过滤源地址，所以，需要使用扩展的 IP 访问列表来满足企业的特殊需求。

- 访问列表位置

应当将扩展 IP 访问列表尽量放在靠近过滤源的位置，这样创建的过滤器就不会反过来影响其他接口上的数据流。而标准访问 IP 列表则应当尽量靠近目的地位置。由于标准 IP 访问列表只使用源地址，因此将阻止报文流向其他端口。

- 语句的位置

由于 IP 协议包含 ICMP、TCP 和 UDP，所以应当将具体的表项放在不太具体的表项前面，以保证位于另一个语句前面的语句不会否定表中后面语句的作用效果。

- 访问列表应用

使用 Access-group 命令应用访问列表。需要注意的是，只有访问列表被应用于接口上时，才执行过滤操作，从而真正产生作用。

- 过滤方向

通过接口的数据流是双向的。过滤方向定义了欲检查的是流入还是流出的报文。所以，访问列表要应用到接口的特定方向上。向外的（outbound）表示数据流从三层设备流出；向内的（inbound）表示数据流流向三层设备。

4. 访问列表配置步骤

① 分析需求，找清楚需求中要保护什么或控制什么；为方便配置，最好能以表格形式列出。

② 分析符合条件的数据流的路径，寻找一个最适合进行控制的位置。

③ 编写 ACL，并将 ACL 应用到接口上。

④ 测试并修改 ACL。

6.7.2 创建并应用 IP 访问列表

1. 创建标准 IP 访问列表

① 进入全局配置模式。

```
Switch# configure terminal
```

② 使用源地址或通配符定义标准 IP 访问列表。

```
Switch(config)# access-list access-list-number {deny | permit} source [source-wildcard]
```

access-list-number ACL 号。相同的所有 ACL 形成一个组。在判断一个包时，使用同一组中的条目从上到下逐一进行判断，一遇到满足的条目就终止对该包的判断。1～99 或 1300～1999 为标准的 IP ACL 号。

deny | permit 当条件匹配时，确定是允许包通过，还是将包丢弃。

Source 源地址。发送包的网络或主机地址，使用点分十分进制数表示。当表示一组主机时，使用通配符屏蔽码。

source-wildcard 通配符屏蔽码。Cisco 访问列表所支持的通配符屏蔽码与子网掩码的方式是相反的。也就是说，二进制数“0”表示一个匹配条件，“1”表示一个不关心条件。

Any 表示任何主机。源地址和源通配符 0.0.0.0 255.255.255.255 的缩写。例如，若欲拒绝

从源地址 192168.1.100 发出的报文，但又允许发自其他源地址的报文，应当使用下述语句：

```
Access-list 1 deny host 192.168.1.100
Access-list 1 permit any
```

需要注意这两条语句的顺序。访问列表语句的处理是由上至下的。如果将两个语句顺序颠倒，将 Permit 语句放在 Deny 语句前面，则不能过滤来自主机的报文，因为 Permit 语句允许所有报文通过。访问列表中的语句顺序非常重要，不合理的语句顺序将会在网络中产生安全漏洞，或者使用户不能很好地利用公司的网络策略。

Host 表示一台主机，是源和源通配符 0.0.0.0 的缩写。例如，若欲允许从 192.168.1.200 发出的报文，则应当使用下述语句：

```
Access-list 1 permit 192.168.1.200 0.0.0.0
```

上述语句也可以使用下面的语句代替：

```
Access-list 1 permit host 192.168.1.200
```

③ 返回特权配置模式。

```
Switch(config)# end
```

④ 校验当前设置。

```
Switch# show access-lists number
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

使用“no access-list *access-list-number*”全局配置命令，可以删除全部访问列表。需要注意的是，不能从指定的访问列表中删除某个 ACE。

2. 创建 IP 扩展访问列表

标准 IP 访问列表只能控制源 IP 地址，不能控制到端口。若欲控制企业用户的网络应用，就需要使用扩展 IP 访问列表。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 定义扩展 IP 访问列表，取值范围为 100～199 或 2000～2699。

```
Switch(config)# access-list access-list-number {deny | permit} protocol source source-wildcard [operator port] destination destination-wildcard [operator port]
```

或者

```
access-list access-list-number {deny | permit} protocol any [operator port] any [operator port]
```

或者

```
access-list access-list-number {deny | permit} protocol host source [operator
```

```
port] host destination [operator port]
```

protocol 欲过滤的协议，如 IP、TCP、UDP、ICMP 等。默认过滤所有协议，若欲根据特殊协议进行报文过滤，需指定协议。

destination destination-wildcard 目的地址和通配符屏蔽码。

operator 端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较。支持的比较操作有：等于（eq）、大于（gt）、小于（lt）、不等于（neq）或介于（range）。如果操作符为 range，则后面需要跟两个端口。

port 端口号，可以用几种不同方法指定。可以显式地指定数字或使用一个可识别的助记符。例如，可以使用 80 或 http 指定超文本传输协议，使用 21 或 ftp 指定文件传输协议。例如，若欲允许来自任何地址的包含有 SMTP 数据的报文到达 192.168.10.10 主机，可以在访问列表中添加下述语句。

```
Access-list 101 permit tcp any host 192.168.10.10 eq smtp
```

③ 返回特权配置模式。

```
Switch(config)# end
```

④ 校验当前设置。

```
Switch# show access-lists number
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

3. 创建命名 IP 访问列表

命名 IP 访问列表有两个主要优点：一是可以解决 ACL 号码不足的问题；二是可以自由地删除 ACL 中的一条语句，而不必删除整个 ACL。而主要不足之处在于无法实现在任意位置加入新的 ACL 条目。

■ **创建命名标准 IP 访问列表**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 利用名称定义标准 IP 访问列表，进入访问列表配置模式。名称可以是 1～99。

```
Switch(config)# ip access-list standard name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-std-nacl)# deny {source [source-wildcard] | host source | any}
```

或者

```
Switch(config-std-nacl)# permit {source [source-wildcard] | host source | any}
```

④ 返回特权配置模式。

```
Switch(config-std-nacl)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

■ **创建命名扩展 IP 访问列表**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 利用名称定义扩展 IP 访问列表，进入访问列表配置模式。名称可以是 100～199。

```
Switch(config)# ip access-list extended name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-ext-nacl)# {deny | permit} protocol {source [source-wildcard]
| host source | any} {destination [destination-wildcard] | host destination | any}
```

④ 返回特权配置模式。

```
Switch(config-std-nacl)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

例如，借助扩展 IP 访问列表，可以在 VLAN 或端口上阻止蠕虫端口，从而避免蠕虫在网络中的蔓延，保证网络的传输效率。

```
access-list 110 deny  tcp any any eq 135
access-list 110 deny  tcp any any eq 445
access-list 110 deny  tcp any any eq 593
access-list 110 deny  tcp any any eq 1029
access-list 110 deny  tcp any any eq 4444
access-list 110 deny  tcp any any eq 5000
access-list 110 deny  tcp any any eq 5554
access-list 110 deny  tcp any any eq 7955
access-list 110 deny  tcp any any range 9995 9996
access-list 110 deny  udp any any range netbios-ns netbios-dgm
access-list 110 deny  udp any any eq tftp
access-list 110 deny  udp any any range 995 999
access-list 110 deny  udp any any eq 1434
access-list 110 deny  udp any any eq 8998
access-list 110 permit ip any any
```

然后，再将该访问列表应用至端口或 VLAN，在入和出双向上启用该列表。

```
ip access-group 110 in
ip access-group 110 out
```

4. 基于时间的访问列表

借助基于时间的访问列表，可以控制用户在某个时间段的访问权限。使用时间访问列表，可以获得以下帮助：

- 借助于允许或拒绝，可以更多地获得对用户访问资源的访问控制，如对某个应用的访问控制（通过 IP 地址、子网掩码和端口号）
- 可以控制日志消息。ACL 表项能够设置为只在每天的某个特定的时间记录通信。这样，就可以简单地忽略高峰时段的通信，从而无需更多地分析日志消息。

基于时间的 ACL 会触发 CPU 动作，因为 ACL 中的新配置必须联合其他特性和配置一起载入物理内存。因此，必须小心配置 ACL，以保证对系统性能的影响最小。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为指定的时间范围命名一个有意义的名称。名称不能包括空格和引号，并且必须以字母开头。

```
Switch(config)# time-range time-range-name
```

③ 指定时间范围。

```
Switch(config-time-range)# absolute [start time date] [end time date]
```

或者

```
periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm
```

或者

```
periodic {weekdays | weekend | daily} hh:mm to hh:mm
```

absolute 指定绝对时间范围。该关键字之后紧跟着 start 和 end 关键字。若欲访问列表中相关的 permit 或 deny 语句生效，则 start 和 end 之后应当紧跟开始和结束的时间。需要注意的是，时间以 24 小时格式表示，日期以“日/月/年”格式表示。

periodic 尽管每个时间范围只能有一个 **absolute** 语句，但却可以有多个 **periodic** 语句。另外，**absolute** 语句只拥有开始和结束时间，以及日期等少数几个参数，而 **periodic** 语句可以使用大量参数，范围可以是一星期中的某一天或几天的组合，或者使用关键字 daily、weekdays 和 weekend 等。表 6-13 列出了在语句中可以使用的一周日期天数的参数。

表 6-13 periodic 语句中可以使用的一周日期天数的参数

参　数	意　义
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	某一天或某几天的组合
daily	从星期一至星期天
weekdays	从星期一至星期五
weekend	星期六和星期日

④ 返回特权配置模式。

```
Switch(config-time-range)# end
```

⑤ 校验当前设置。

```
Switch# show time-range
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

例如，若欲限制所有员工在周一至周五的8:00～18:00使用QQ和MSN聊天，可以在访问列表中添加下述语句：

```
time-range deny-qq
!---定义时间范围名称为“deny-qq”
periodic weekdays start 8:00 end 18:00
!---时间范围为周一至周五的8:00～18:00
ip access-list extend internet_limit
!---定义扩展IP访问列表，名称为“qq_limit”
deny tcp 10.1.0.0 0.0.255.255 any eq 1863 time-range deny-qq
deny tcp 10.1.0.0 0.0.255.255 any eq 8000 time-range deny-qq
deny tcp 10.1.0.0 0.0.255.255 any eq 1080 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 8000 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 4000 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 1080 time-range deny-qq
!---定义QQ和MSN聊天使用的协议和端口号
permit ip any any
!---其余访问不予限制
```

需要注意的是，网络应用程序所使用的端口号，大多都可以在下述下文件中找到。

```
Win9x:%windir%\services
WinNT/2000/XP：%windir%\system32\drivers\etc\services
Linux：/etc/services
```

如果在services文件中找不到端口的应用，可以在运行程序前后，运行netstat－ap比较并找出应用所使用的端口号。

5. 将IP访问列表应用到接口

■ IPv4 ACL与网络接口

如果不将IP访问列表应用到接口，那么该访问列表将不会发生作用。在将ip access-group接口配置命令应用于三层接口（如SVI、三层EtherChannel或路由端口）时，接口必须配置有IP地址。三层访问组只过滤CPU处理的三层路由或接收到的包，而不会对VLAN中的桥接产生影响。

对入站（inbound）ACL而言，交换机在接收到包后先进行检查。如果ACL允许该包，交换机继续处理该包；如果ACL拒绝该包，则交换机丢弃该包。

对于出站（outbound）ACL而言，在接收或路由包到控制接口之后进行检查。如果ACL允许该包，则交换机发送该包；如果ACL拒绝该包，而交换机丢弃该包。

默认情况下，每当包被丢弃，入口将发送ICMP不可到达消息，无论引发这个丢弃动作的是入口上ACL的原因，还是出口上ACL的原因。ICMP不可到达消息被限制在最多每半秒在

每个接口上发送一次。

当将没有限制的 ACL 应用于接口时，交换机将视为没有 ACL 应用于接口，并且允许所有的包传输。在为保障网络安全而配置 ACL 时，一定要切记这一点！

在将 IPv4 ACL 应用于网络接口时，应当注意以下几点：

- 当控制一个接口的访问时，可以使用命名或序号 ACL。
- 将 ACL 应用至作为 VLAN 成员的二层接口时，二层（端口）ACL 优先于应用于 VLAN 接口的输入三层 ACL，或应用于 VLAN 的 VLAN 映射。
- 如果应用 ACL 至三层接口，并且交换机上的路由未被启用，ACL 只为 CPU 过滤包，如 SNMP、Telnet 或 Web 通信。
- 不要在应用至二层接口的 ACL 启用路由。

■ **配置过程**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲应用该 IP 访问列表的接口。该接口既可以是二层接口（端口访问列表），也可以是三层接口（路由访问列表）。

```
Switch(config)#interface interface-id
```

③ 将访问控制应用到指定的接口。二层接口（端口访问列表）不支持 out 关键字。

```
Switch(config-if)# ip access-group {access-list-number | name} {in | out}
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 校验当前设置。

```
Switch# show running-config
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

6.7.3 创建并应用 MAC 访问列表

在 VLAN 或二层接口上，可以使用 MAC 地址和 MAC 扩展 ACL 名称过滤非 IP 地址通信，从而保障企业网络访问安全，拒绝非授权用户对敏感部门的访问。配置过程与其他扩展名称 ACL 相似。

1. 创建命名 MAC 扩展访问列表

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为扩展 MAC 地址列表定义一个名称，进入扩展 MAC 地址列表配置模式。

```
Switch(config)# mac access-list extended name
```

③ 定义允许或拒绝的源 MAC 地址或目的 MAC 地址。使用 Host，可以指定特定主机的 MAC 地址；使用掩码，可以指定多个主机的 MAC 地址。

```
Switch (config-ext-mac)# {deny | permit} {any | host source MAC address | source MAC address mask} {any | host destination MAC address | destination MAC address mask}
```

④ 返回特权配置模式。

```
Switch(config-ext-mac)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

2. 将 MAC 访问列表应用到二层接口

创建 MAC ACL 后，可以将其应用至二层接口，以过滤到达该接口的非 IP 通信。在应用 MAC ACL 时，应当考虑以下几点：

- 如果应用 ACL 的二层接口是 VLAN 成员，二层（端口）ACL 优先应用于 VLAN 接口的三层 ACL（输入方向），或应用于该 VLAN 的 VLAN 映射。二层端口接收到的进入的包总是要以端口 ACL 进行过滤。
- 可以应用多个 IP 访问列表和一个 MAC 列表至同一个二层接口。IP 访问列表只过滤 IP 包，MAC 访问列表则过滤非 IP 包。
- 二层接口只能有一个 MAC 访问列表。如果应用一个 MAC 访问列表到已经配置有 MAC ACL 的二层接口，新的 ACL 将替换较早前的配置。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲应用该 IP 访问列表的二层接口。

```
Switch(config)#interface interface-id
```

③ 将 MAC 访问列表应用到二层接口。注意，该命令不适用于 EtherChannle。

```
Switch(config-if)# mac access-group {name} {in | out}
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 校验当前设置。

```
Switch# show mac access-group [interface interface-id]
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

6.7.4 创建并应用 VLAN 映射

vlan-map 是 vlan 中的一种访问控制应用。创建和应用 VLAN 映射至 VLAN 的大致过程是：创建欲应用于 VLAN 的标准或推展 IPv4 ACL，或者命名 MAC 扩展 ACL；使用 vlan access-map 的全局命令创建一个 vlan-map；使用 match 命令指定需要匹配的 IP 和 MAC 通信；使用 action 命令设置匹配后 IP 包或非 IP 包（只有一个已知的 MAC 地址）数据包的处理是转发还是丢弃；使用 vlan filter 命令对通信进行过滤。

1. VLAN 映射配置策略

VLAN 映射是 VLAN 中控制过滤的唯一途径。VLAN 映射没有方向，因此，若欲在使用 VLAN 映射时指定方向过滤通信，需要包含一个指定源和目的地址的访问列表。如果在 VLAN 映射中有过滤包类型（IP 或 MAC）的匹配语句，那么，当一个包不匹配其中的任何表项时，默认的动作就是丢弃。如果没有包类型的匹配语句，则默认转发。

在配置 VLAN 映射时，应当遵循以下策略：

- 如果在接口上没有配置 ACL 禁止通信，并且配置有 VLAN 映射，那么，所有通信都被允许。
- 每个 VLAN 映射都由一系列的表项组成，这意味着其中的每个表项都很重要。进入交换机的包首先与 VLAN 映射中的第一个表项进行匹配，如果匹配，指定的动作就会发生。如果不匹配，将与 VLAN 映射中的下一个表项再次进行匹配。
- 如果 VLAN 映射中有至少一个包类型（IP 或 MAC）匹配语句，如果包不匹配的其中任何一个语句，那么，默认将丢失该包。如果 VPAN 映射中没有包类型的匹配语句，默认将转发该包。
- 日志不支持 VLAN 映射。
- 当交换机有一个 IP 访问列表或 MAC 地址列表应用于二层接口时，再将 VLAN 映射应用于属于该 VLAN 的端口时，包访问列表优先于 VLAN 映射。
- 如果硬件中的 VLAN 映射配置没有被应用，VLAN 中的所有包都将被丢弃。

2. VLAN 映射和路由访问列表配置策略

以下配置策略在同一 VLAN 同时配置路由访问控制列表和 VLAN 映射时适用，不适用于在不同 VLAN 应用路由访问控制列表和 VLAN 映射的配置。如果必须在同一 VLAN 配置路由 ACL 和 VLAN 映射，那么，路由 ACL 和 VLAN 映射配置必须遵循以下准则：

- 在 VLAN 接口的每个方向（input/output），只能配置一个 VLAN 映射和一个路由 ACL。
- 无论如何，除非在最后，否则，不要编写所有表项只有一个动作的 ACL，且该动作默认为其他类型。换句话说，编写 ACL 时，应当使用下列结构中的任何一个，即：permit... permit...permit... deny ip any any，或者，或者 deny... deny... deny... permit ip any any。
- 在 ACL（permit, deny）中定义多个动作时，应当将每个动作类型组合在一起，以减少表项的数量。

- 在 ACL 中应当避免包括四层信息，添加类似信息将使处理变得复杂化。最佳的处理结果是 ACL 基于 IP 地址（源或目的）进行过滤，并实现非满负荷通信（源 IP 地址、目的 IP 地址、协议、协议端口）。

3. 创建 VLAN 映射

① 进入全局配置模式。

```
Switch# configure terminal
```

② 创建 VLAN 映射，并给该 VLAN 访问列表定义一个名称和序号，进入 VLAN 访问列表配置模式。当创建的 VLAN 映射名称相同时，其序号将会以 10 为增量增加。需要修改和删除映射时，可以直接指定其序号。VLAN 映射不能使用 permit 或 deny 关键字。若欲使用 VLAN 映射阻止包，需要创建一个 ACL 来匹配包，并且将动作设置为丢弃。ACL 中的 permit 被认为是匹配，而 deny 则意味着不匹配。

```
Switch(config)# vlan access-map name [number]
```

③ 借助一个或多个标准或扩展访问列表匹配包（使用 IP 或 MAC 地址）。需要注意的是，包只能与适当协议类型的访问列表相匹配，即 IP 包只能被标准或扩展 IP 访问列表匹配，非 IP 包只能被 MAC 扩展访问列表匹配。

> **注·意** 如果 VLAN 映射被配置为包类型（IP 或 MAC）匹配语句，并且映射动作为丢弃，那么，匹配类型的所有包都将被丢弃。如果 VLAN 映射没有匹配语句，并且设置动作为丢弃，那么，所有 IP 和第二层包都将被丢弃。

```
Switch (config-access-map)# match {ip | mac} address {name | number} [name | number]
```

④ 为 VLAN 映射设置动作，默认为转发（forward）。

```
Switch (config-access-map)# action {drop | forward}
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 校验当前设置。

```
Switch# show running-config
```

⑦ 保存当前配置。

```
Switch# copy running-config startup-config
```

4. 将 VLAN 映射应用到 VLAN

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将 VLAN 映射应用至一个或多个 VLAN。可以使用“-”或“,”指定若干 VLAN。需要注意的是，“-”或“,”前后必须键入空格。

```
Switch(config)# vlan filter mapname vlan-list list
```

③ 校验当前设置。

```
Switch# show running-config
```

④ 保存当前配置。

```
Switch# copy running-config startup-config
```

6.8 其他重要配置

6.8.1 配置 DHCP 中继

如果一个网络包含有多个子网，或划分为多个 VLAN，但网络内却只有一个 DHCP 服务器，那多个网段就不能使用同一个 DHCP 服务器了。虽然可以通过在每个网段都添加一个 DHCP 服务器，但这样不仅成本高，而且不便于管理。而使用 DHCP 中继代理，就可以使各个网段的 DHCP 请求都能发送到 DHCP 服务器，并且各个网段都能使用 DHCP 功能。

1. DHCP 中继代理概述

由于 DHCP 依赖于广播信息，因此一般情况下应将 DHCP 客户机和 DHCP 服务器设置于同一网段之内。而对于多个网段向 DHCP 请求 IP 地址时，由于 DHCP 不能跨网段操作，所以最好在某个网段中部署两台或更多的 DHCP 服务器，而在其他网段使用 DHCP 中继代理。

使用 DHCP 中继代理，可以使 DHCP 请求能够从一个网段传递到另一个网段，但必须遵循以下要求。

- 在路由网络里，一个 DHCP 服务器必须至少位于一个网段中。
- 必须使用路由器或计算机作为 DHCP 和 BOOTP 中继代理服务器以支持网段之间的 DHCP 通信的转发。

不同网段依靠路由设备连接，而路由设备本身会阻断 LAN 广播，这样，没有部署 DHCP 服务器的网段就无法向部署有 DHCP 服务器的网段发出 DHCP 地址请求。要解决这个问题，需要添加一个 DHCP 中继代理服务器（如图 6-5 所示），当有 DHCP 服务器的网段中的客户机发出 DHCP 请求时，DHCP 中继代理就会像 DHCP 服务器一样接收广播，然后向另一网段的 DHCP 服务器发出单播请求，这样就可以获得 IP 地址了。

DHCP 中继代理有两种解决方案。其一，路由设备（含三层交换机）必须支持 DHCP/BOOTP 中继代理功能（符合 RPC 1542 规范），能够中转 DHCP 和 BOOTP 通信。当然，目前绝大多数路由器或三层交换机都支持 DHCP 中继代理。其二，在一台运行 Windows Server 2003/2008 的服务器上安装 DHCP 中继代理组件，并配置 DHCP 代理。

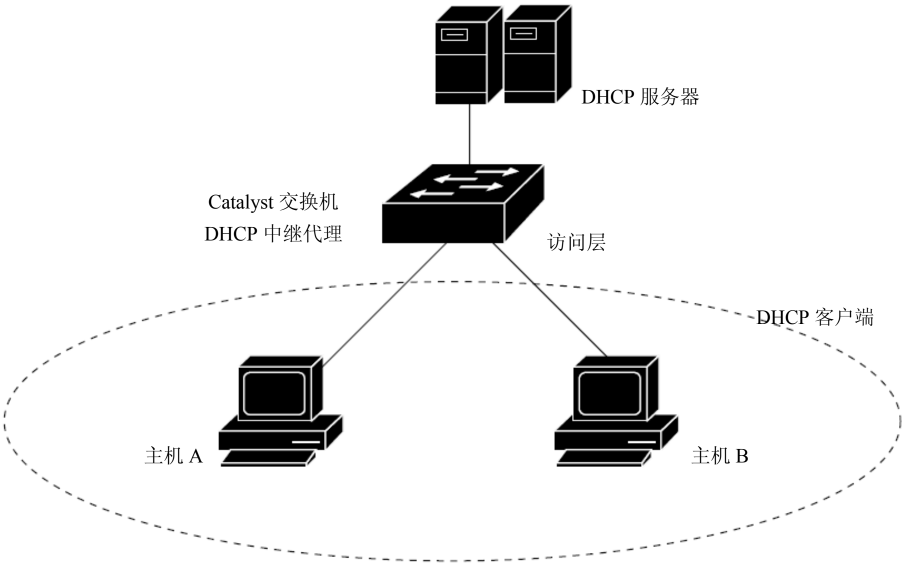


图 6-5　DHCP 中继代理服务器

> **提·示**　当然，若欲为网络客户端自动分配 IP 地址，必须安装 DHCP 服务器。有关 DHCP 服务器搭建和管理的内容，请参见《Windows Server 2008 组网技术详解(服务器搭建与升级篇)》(电子工业出版社，张栋 刘晓辉 编著，2010 年 2 月)。

2.　DHCP 默认配置

表 6-14 列出了 DHCP 的默认配置。

表 6-14　DHCP 默认配置

特　　征	默认设置
DHCP 服务	在 Cisco IOS 软件中被启用，需要配置
DHCP 中继代理	启用
DHCP 包转移地址	未配置
查询中继代理信息	启用
DHCP 中继代理转移规则	替代已存在的中继代理信息
DHCP 全局监测	禁用
DHCP 选项信息监测	启用
DHCP 侦听选项接受不信任输入端口的包	禁用
DHCP 侦听限速	未配置
DHCP 侦听信任	不信任
DHCP 侦听 VLAN	禁用
DHCP 侦听 MAC 地址确认	启用
Cisco IOS DHCP 服务器绑定数据库	在 Cisco IOS 软件中被启用，但需要配置
DHCP 监测绑定数据库代理	在 Cisco IOS 软件中被启用，但需要配置

3.　DHCP 配置策略

DHCP 侦听配置策略方针如下。

- 必须在交换机上启用全局 DHCP 侦听。
- 在 VLAN 上启用之后，DHCP 侦听才有效。
- 在交换机上启用全局 DHCP 侦听之前，务必保证 DHCP 服务器运行的设备和 DHCP 中继代理已经配置并启用。
- 当交换机上启用全局 DHCP 侦听时，如果侦听有效，Cisco IOS 指令就可以得到。如果使用这些指令，交换机会返回一个错误信息，并且这些配置将不会被应用。

① ip dhcp relay information check global configuration command

② ip dhcp relay information policy global configuration command

③ ip dhcp relay information trust-all global configuration command

④ ip dhcp relay information trusted interface configuration command

- 在交换机上配置 DHCP 侦听信息选项之前,确保配置了作为 DHCP 服务器运行的设备。
- 当在交换机上配置大量的链路标识时，要考虑到 NVRAM 字符串的长度或者闪存的容量。如果链路标识和其他的数据配置混合在一起，超出了 NVRAM 或者闪存的容量，就会出现错误信息。
- 在交换机上配置 DHCP 中继代理之前，确保配置了作为 DHCP 服务器运行的设备。
- 如果 DHCP 中继代理启用，但是 DHCP 侦听禁用，则不支持 DHCP option-82 数据插入特性。
- 如果交换机端口连接到 DHCP 服务器，输入“ip dhcp snooping trust”接口配置指令来配置可信任端口。
- 如果交换机端口连接到 DHCP 客户端，输入“no ip dhcp snooping trust”接口配置指令来配置不可信任端口。
- 当 DHCP 侦听绑定数据库时的配置方针时：

① 因为 NVRAM 和闪存都有存储容量的限制，建议在 TFTP 服务器上存储这些绑定文件。

② 基于网络的 URL（像 TFTP 和 FTP），在交换机写入绑定信息到那个 URL 中的绑定文件之前，必须在已经配置好的 URL 上创建一个空的文件。TFTP 服务器查看这个文件决定是否要首先在服务器上创建一个空文件，一些 TFTP 服务器不能用这种方式配置。

③ 确保数据库的租赁时间是准确的，建议启用并配置 NTP。

④ 如果已经配置好了 NTP，只要当交换机系统时钟与 NTP 一同使用时，交换机便将绑定改变写入绑定文件。

4. 配置 DHCP 中继代理

当服务器与客户端跨越 VLAN 和子网时，必须配置 DHCP 中继代理。由于所有 Cisco 二层和三层交换机都支持 DHCP 代理，因此只需进行简单设置，即可实现跨 VLAN 的 DHCP 服务。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 在交换机上启用 DHCP 服务和中继代理。默认状态下，该功能被启用。

```
Switch(config)# service dhcp
```

提·示　如果 DHCP 服务器和 DHCP 客户端在不同的网络或子网，那么就必须使用 ip helper-address *address* 接口配置命令设置交换机。通常情况下，在离客户端最近的三层交换机上配置该命令。使用 ip helper-address 命令，可以指定服务器的 IP 地址，如果其他 DHCP 服务器在该目的网段，也可能是网络地址。使用网络地址时，可以启用所有 DHCP 服务器的响应请求。

③ 选择配置 DHCP 中继的 VLAN，进入接口配置模式。

```
Switch(config)# interface vlan vlan-id
```

或

```
Switch(config)# interface range vlan-range
```

提·示　配置 DHCP 中继代理之前，应当先创建 VLAN，并为 VLAN 虚拟三层接口指定 IP 地址信息。有关 VLAN 和 IP 地址信息的配置方式，请参见本章上述相关内容。

④ 指定 DHCP 包转发地址。helper-address 可以指定为 DHCP 服务器地址，或者默认网关的地址（如果 DHCP 服务器位于另外的网关）。使用网关地址，可以使 DHCP 服务器能够响应 DHCP 请求。如果网络内安装有多台 DHCP 服务器，可以为每台服务器分别配置一个 helper address。DHCP 服务器所在的 VLAN 不必指定 helper address。

```
Switch(config-if)# ip helper-address address
```

提·示　通常情况下，必须为每个 VLAN 都配置 DHCP 中继代理。否则，客户端将不能自动获取 IP 地址信息。

⑤ 返回全局配置模式。

```
Switch(config-if)# end
```

⑥ 校验配置。

```
Switch# show running-config
```

⑦ 保存当前配置。

```
Switch# copy running-config startup-config
```

6.8.2 配置 HSRP

HSRP（Hot Standby Router Porctocol，热备份路由协议）的目的在于使主机看上去只使用

了一个路由器，并且即使在它当前所使用的首跳路由器失败的情况下仍能够保持路由的连通性。此协议中所涉及到的多路由器都映射为一个虚拟的路由器，保证同时有且只有一个路由器在代表虚拟路由器进行包的发送，而终端则是把数据包发向该虚拟路由器。

1. HSRP 默认配置

HSRP 的默认配置如表 6-15 所示。

表 6-15　HSRP 的默认设置

特　　性	默认设置
HSRP 版本	版本 1
HSRP 组	未配置
备份组号	0
备份 MAC 地址	系统分配为：0000.0c06.acXX，XX 是 HSRP 组号
备份优先权	100
备份延迟	0（无延迟）
备份追踪接口优先权	10
备份 hello 时间	3 s
备份 holdtime	10 s

2. HSRP 配置策略

下面是配置 HSRP 的一些配置策略。

- HSRP v2 和 HSRP v1 相互具有排他性。在一个接口上 HSRP v2 和 HSRP v1 彼此不能协作。
- HSRP 最多可以在 32 个 VLAN 或者路由接口上配置。
- 指定接口必须是三层接口。

① 路由器端口。将一个物理端口配置为三层接口，键入“no switchport”接口配置命令。

② SVI（Switch Virtual Interface，交换机虚拟接口）。创建一个 VLAN 接口，使用“interface vlan vlan_id”全局配置指令，也可以使用三层默认接口。

③ 三层 Etherchannel 接口（Port Channel）。使用“interface port-channel port-channel-number”全局配置命令，将以太网接口绑定到 Channel 组来创建 port-channel 逻辑接口。

- 所有三层接口都必须分配 IP 地址。
- 当组号小于 256 时，HSRP 组的版本可以从 HSRP v2 改变为 HSRP v1。
- 当改变某个接口的 HSRP 版本时，每个 HSRP 组都要重新配置，因为其拥有了新的虚拟 MAC 地址。

3. 启用 HSRP

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置 HSRP 的三层接口，进入接口配置模式。

```
Switch(config)# interface interface_id
```

③（可选）在接口上配置 HSRP 版本。1 表示采用 HSRP v1，2 表示采用 HSRP v2。

```
Switch(config-if)# standby version {1 | 2}
```

④ 使用组号和虚拟 IP 地址创建 HSRP 组。（可选）group-number，指定该接口上启用的 HSRP 组号，取值范围为 0～255，默认值为 0。如果只有一个 HSRP 组，则不必键入组号。（可选）ip-address，热备份路由接口的虚拟 IP 地址。必须为这些接口至少键入一个虚拟 IP 地址，它可以从其他接口学到。Secondary，表示该 IP 地址是次热备份路由接口。如果既没有指定作为次备份路由或备份路由，也没有设置优先级，主 IP 地址将进行比较并把拥有较高 IP 地址的路由作为活跃路由，下一个较高的作为备份路由。

```
Switch(config)# standby [group-number] ip [ip-address [secondary]]
```

⑤ 返回特权 Exec 模式。

```
Switch(config)# end
```

⑥ 校验配置。

```
Switch # show standby [interface_id [group]]
```

⑦ 保存配置。

```
Switch(config)# copy running-config startup-config
```

使用“**no standby** [*group-number*] **ip** [*ip-address*]”接口配置指令来禁用 HSRP。

4. 配置 HSRP 优先级

■ **配置策略**

在配置 HSRP 优先级时，应当遵循以下策略。

- 通过指定优先级，可以选择活跃路由和备份路由。当优先权（Preemption）被启用时，拥有较高优先级的路由将变成活跃路由。如果优先级相同，当前活跃路由不会改变。
- 较高的数字（1～255）表示较高的优先级，更有希望变成活跃路由器。
- 当设置优先级（priority）、优先权（preempt）或同时设置两者（both）时，必须指定至少一个关键字（priority、preempt 或两者）。
- 如果接口使用 standby track 命令配置时，设备的优先级可以动态改变，该路由上的其他接口将宕掉（down）。
- 当在接口上第一次启用路由时，没有完整的路由表。如果将其配置为 Preempt，那么，该路由将改变为活跃路由，即使它还不能提供适当的路由服务。若欲解决这个问题，可以配置一个延迟时间，以允许路由器有时间更新其路由表。

■ **配置命令**

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置 HSRP 优先级的接口，进入接口配置模式。

```
Switch(config)# interface interface_id
```

③ 设置用于选择活跃路由器的优先级。priority 取值范围是 1～255，默认值为 100。数值越高，优先权越高。group-number，（可选）指定命令适用的 HSRP 组号。preempt，（可选）选择当本地路由比活跃路由拥有较高优先级时，将作为活跃路由进行控制。delay，（可选）设置本地路由延迟接管活跃规则的时间，单位为秒，取值范围为 0～3 600，默认值为 0（接管前没有延迟）。

```
Switch(config-if)# standby [group-number] priority priority [preempt [delay delay]]
```

④ 配置路由器优先权（preempt）。当本地路由器比活跃路由器拥有更高的优先级时，将作为活跃路由器。group-number，（可选）指定命令适用的 HSRP 组号。Priority，设置或修改组优先级，取值范围为 1～255，默认值为 100。delay，（可选）设置本地路由延迟接管活跃规则的时间，单位为秒，取值范围为 0～3 600，默认值为 0（接管前没有延迟）。

```
Switch(config-if)# standby [group-number] [priority priority] preempt [delay delay]
```

⑤ 配置一个接口来追踪其他接口。一旦其他接口宕掉，那么，该设备的热备份优先级即被降低。group-number，（可选）指定命令适用的 HSRP 组号。*Type number*，指定被追踪接口的类型和接口号。*interface-priority*，（可选）指定当接口宕掉或从备份中恢复时，路由的热备份优先级减少或增加的总值，默认值为 0。

```
Switch(config-if)# standby [group-number] track type number [interface-priority]
```

⑥ 返回特权 Exec 模式。

```
Switch(config-if)# end
```

⑦ 校验配置。

```
Switch# show running-config
```

⑧ 保存配置。

```
Switch # copy running-config startup-config
```

使用"**no standby** [*group-number*] **priority** *priority* [**preempt** [**delay** *delay*]]"和"**no standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** *delay*]"接口配置指令，重新配置默认优先级、优先权和延迟值。

使用"**no standby** [*group-number*] **track** *type number* [*interface-priority*]"接口配置指令移除追踪。

6.8.3 配置 802.1x 基于端口的认证

IEEE 802.1x 身份验证用于对有线以太网和无线 IEEE 802.11 网络进行经过身份验证的网络访问。IEEE 802.1x 通过提供对集中式用户标识、身份验证、动态密钥管理和计账的支持来提高安全性和部署。IEEE 802.1x 执行基于端口的网络访问控制。基于端口的网络访问控制使用交换的局域网基础设施的物理特征来验证连接到 LAN 端口的设备，并防止访问身份验证进

程已经失败的那个端口。若欲实现 IEEE 802.1x 认证，必须在 Cisco 交换机上作必要的配置。

1. IEEE 802.1x 简介

以太网技术“连通和共享”的设计初衷使目前由以太网构成的网络系统面临很多安全问题。IEEE 802.1x 协议正是基于这样的背景下被提出来的，成为解决局域网安全问题的一个有效手段。

在 802.1x 协议中，只有具备了以下 3 个要素（如图 6-6 所示）才能够完成基于端口的访问控制的用户认证和授权。

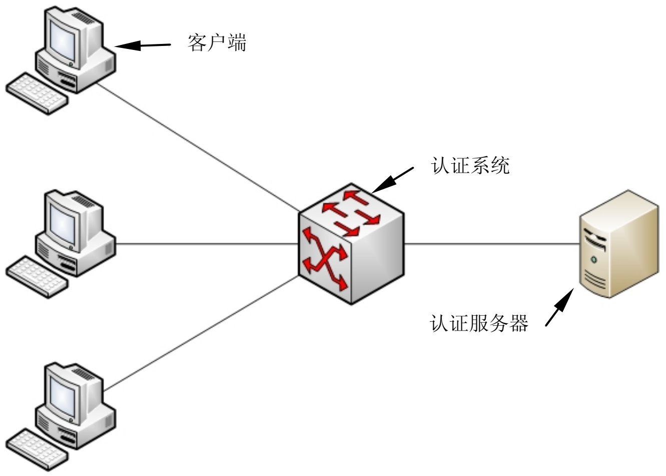


图 6-6　802.1x 协议认证三要素

- 客户端：一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。
- 认证系统：在以太网系统中指认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。
- 认证服务器：通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

提示

对于由 Cisco 设备搭建的局域网而言，建议使用专业的 Cisco ACS 作为认证服务器。Cisco ACS 可以与 Windows Server 2003/2008 活动目录很好地联合工作，从而使得 Windows 用户认证与 Cisco 网络访问有机地整合在一起。用户只需使用一套用户名和密码，即可实现对局域网络（甚至是 VPN）的访问，并获得相应的访问权限。

在具有 802.1x 认证功能的网络系统中，当一个用户需要对网络资源进行访问之前必须先要完成以下认证过程（如图 6-7 所示）。

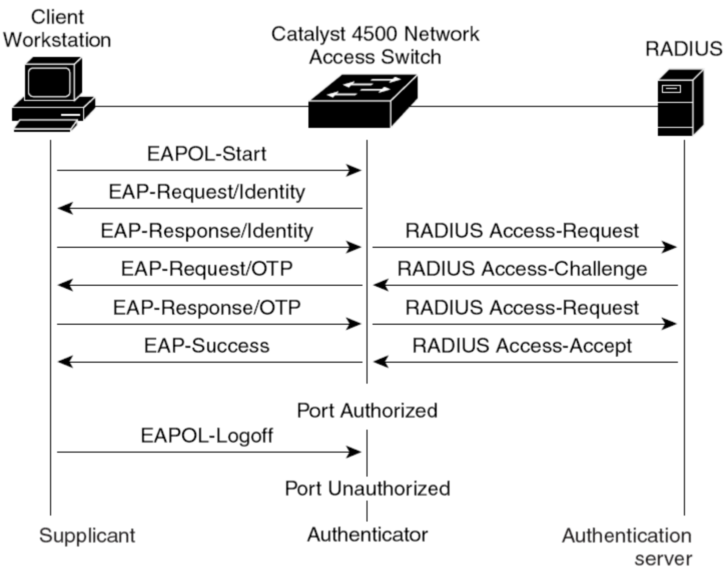


图 6-7　802.1x 认证过程

（1） 当用户有上网需求时打开 802.1x 客户端程序，输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

（2） 交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名传送上来。

（3） 客户端程序响应交换机发出的请求，将用户名信息通过数据帧传送给交换机。交换机将客户端传送上来的数据帧经过封包处理后再传送给认证服务器进行处理。

（4） 认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

（5）客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理（此种加密算法通常是不可逆的），并通过交换机传给认证服务器。

（6） 认证服务器将传送上来的加密后的口令信息和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的命令，允许用户的业务流经过端口访问网络。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

2. 启用 IEEE 802.1x 认证

借助以下操作，可以在指定的交换机上启用 IEEE 802.1x 认证，实现用户登录认证。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 在交换机上启用 IEEE 802.1x 认证。

```
Switch(config)# dot1x system-auth-control
```

③ 启用AAA。

```
Switch(config)# aaa new-model
```

④ 创建IEEE 802.1x AAA认证方式列表。如果在认证命令中没有指定列表名称，将创建并使用一个默认列表。默认情形下，将使用认证方式后的默认关键字。默认认证方式自动应用于所有接口。键入至少一个关键字：group radius意为使用列表中所有的RADIUS服务器认证；none意为不认证，客户端自动通过交换机认证，而无需使用客户端支持信息。

```
Switch(config)# aaa authentication dot1x {default} method1 [method2...]
```

⑤ 指定欲启用IEEE 802.1x认证的端口。

```
Switch(config)# interface interface-id
```

⑥ 将该端口指定为非中继、非标签的单一VLAN 2层接口。

```
Switch(config-if)# switchport mode
```

⑦ 在该端口以默认参数启用802.1x认证。

```
Switch(config-if)# dot1x pae authenticator
Enables 802.1x authentication on the port with default parameters.
```

⑧ 在该端口启用802.1x认证。

```
Switch(config-if)# dot1x port-control auto
```

⑨ 在该端口启用IEEE 802.1x认证。

```
Switch(config-if)# dot1x port-control auto
```

⑩ 返回特权模式。

```
Switch(config-if)# end
```

⑪ 查看配置是否正确。

```
Switch# show dot1x
```

⑫ 保存配置。

```
Switch# copy running-config startup-config
```

> **提·示** 若欲在多个端口启用IEEE 802.1x认证，应当重复指定端口和启用认证的操作。或者将相同配置的端口设置为一个端口组，然后配置该端口组。

3. 配置交换机到RADIUS服务器的通信

Radius 服务器维护了所有用户的信息，包括用户名、密码、该用户的授权信息，以及该

用户的记账信息。所有的用户集中于 Radius Server 管理，而不必分散于每台交换机，便于管理员对用户的集中管理。

RADIUS 安全服务器通过主机名或 IP 地址、主机名和指定的 UDP 端口号，或者 IP 地址和指定的 UDP 端口号而被识别。IP 地址和 UDP 端口号相结合构成唯一的标识符，在一个 IP 地址的服务器上，可以采用多 UDP 端口方式启用多个 RASIUS 请求。如果在同一 RADIUS 服务器上配置两个不同的主机条目，那么第 2 个主机条目将担当第 1 条目失败后的备份。

交换机到 RADIUS 服务器的通信配置如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 配置 RADIUS 服务器参数。hostname | ip-address，指定 RADIUS 服务器的主机名或 IP 地址。auth-port port-number，指定认证请求的 UDP 目的端口。若默认为 1812，可取值范围为 0～65 536。key string，指定在交换机和 RADIUS 服务器之间的认证或加密密钥。这个密钥是一个字符串，必须与 RADIUS 服务器上使用的密钥相匹配。若欲使用多个 RADIUS 服务器，重复键入该命令。

```
Switch(config)# radius-server host {hostname | ip-address} auth-port port-number key string
```

③ 返回特权配置模式。

```
Switch(config-if)# end
```

④ 校验当前设置。

```
Switch# show running-config
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

提示

对于小型网络而言，可以使用 Windows Server 2003 内置的 IAS 服务，或者 Windows Server 2008 内置的 RADIUS 服务充当 RADIUS 服务器。有关 IAS 或 RADIUS 服务的配置，请参见《网络服务器搭建与管理(第 2 版)》(电子工业出版社，刘晓辉 郑凯，2009.3）“第 15 章 VPN 服务”中的相关内容。

4. 配置重新认证周期

可以实施对 802.1x 客户的定期重新认证，并且指定重新认证的周期。默认情况下，两次认证的间隔为 3 600 s。如果人员流动性较大，且对安全性要求较高，可以缩短重新认证的时间。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置的端口。

```
Switch(config)# interface interface-id
```

③ 启用定期重新认证。默认状态下，该功能被禁用。

```
Switch(config-if)# dot1x reauthentication
```

④ 设置两次重新认证之间的时间间隔，单位为秒（s）。取值范围为 1～65 535，默认为 3 600 s。

```
Switch(config-if)# dot1x timeout reauth-period seconds
```

⑤ 返回特权配置模式。

```
Switch(config-if)# end
```

⑥ 校验当前设置。

```
Switch# show dot1x interface interface-id
```

⑦ 保存当前配置。

```
Switch# copy running-config startup-config
```

5. 修改安静周期

所谓安静周期，是指当客户端无法通过认证后，再次认证所需要等待的时间。为了使用户尽快得到再次重新尝试键入密码，以正确登录网络的机会，可以缩短安静周期。当然，应当在一些比较可靠的接口设置。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置的端口。

```
Switch(config)# interface interface-id
```

③ 指定认证失败后，可以重新认证所需等待的时间。默认状态为 60 s，可取值范围为 1～65535 s。

```
Switch(config-if)# dot1x timeout quiet-period seconds
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 校验当前设置。

```
Switch# show dot1x interface interface-id
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

第 7 章　使用 CLI 管理和监控交换机

对于傻瓜交换机而言，所有的管理就是对连接电缆的管理，即连接或终止每个端口所连接的设备。而对于可网管交换机而言，除此之外，还可以通过一些简单的配置，实现网络安全、提高网络通信效率，实现对交换机的远程监控与管理。

7.1　监控交换机

7.1.1　监控交换机系统状态

1.　交换机引导过程

标准引导过程涉及引导装载软件的操作，执行过程如下。

- 执行低级 CPU 初始化。初始化 CPU 寄存器，控制物理内存映射，以及其数量、速率等等。
- 执行 CPU 子系统的加电自检（power-on self-test，POST）。测试 CPU DRAM 和构成 Flash 文件系统的 Flash 设备部分。
- 初始化系统主板上的 Flash 文件系统。
- 将默认操作系统软件映像装载至内存，引导交换机。

在操作系统装载之前，引导装载提供对 Flash 文件系统的访问。一般情况下，引导装载只被用于载入，解压缩和启动操作系统。在引导装载得到 CPU 的操作系统控制权之后，直到下一次系统复位或加电，它将一直处于不活动状态。

如果操作系统的问题严重到不能使用的程度，引导装载也提供进入系统的陷阱访问，可以使用 Xmodem 协议格式化 Flash 文件系统，重新安装操作系统软件映像，恢复遗忘的密码，并重新启动操作系统。

2. 配置在线诊断任务

可以制订详尽的在线诊断任务计划，包括指定的日期和时间、指定的次数，以及在发生错误时进行的动作。

diagnostic schedule test {*test_id* **|** *test_id_range* **| all | basic | non-disruptive}** **{daily** *hh:mm* **| on** *mm dd yyyy hh:mm***} | weekly** *day_of_week hh:mm***}**

3. 配置健康监控诊断

当交换机连接到网络时，可以配置健康监测诊断测试，包括配置每次健康测试的执行间

隔，在测试失败后是否生成系统消息，以及个别测试失败后启用或禁用。

配置指定的健康监测周期。默认情况下，监测是被禁用的。

diagnostic monitor interval test {*test_id* | *test_id_range*} *hour:mm:ss milliseconds day*

健康监测测试失败后是否生成系统日志消息。默认情况下，系统日志消息被禁用。

diagnostic monitor syslog

设置监测测试失败阀值。默认情况下，监测被禁用。

diagnostic monitor threshold test {*test_id* | *test_id_range*} **failure count** *count*

4. 运行在线诊断测试

在线诊断测试能够发现下述问题：

- 硬件组件
- 接口
- 焊点

在指定交换机上启动诊断测试（如图 7-1 所示）。

diagnostic start test {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}

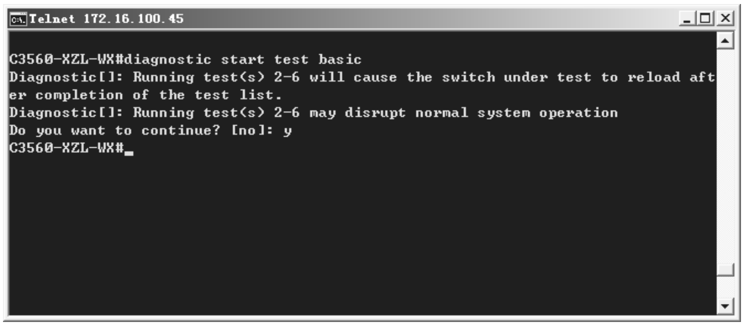


图 7-1　启动诊断测试

显示交换机的在线诊断测试配置（如图 7-2 所示）。

show diagnostic content

显示在线诊断测试是否正在运行。

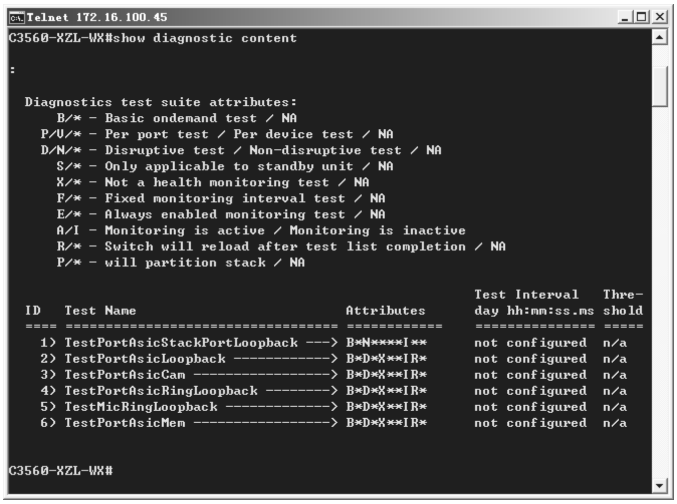
show diagnostic status

显示在线诊断结果。

show diagnostic result detail
show diagnostic result test [*test_id* | *test_id_range*] [**detail**]

显示在线诊断测试任务。

show diagnostic schedule

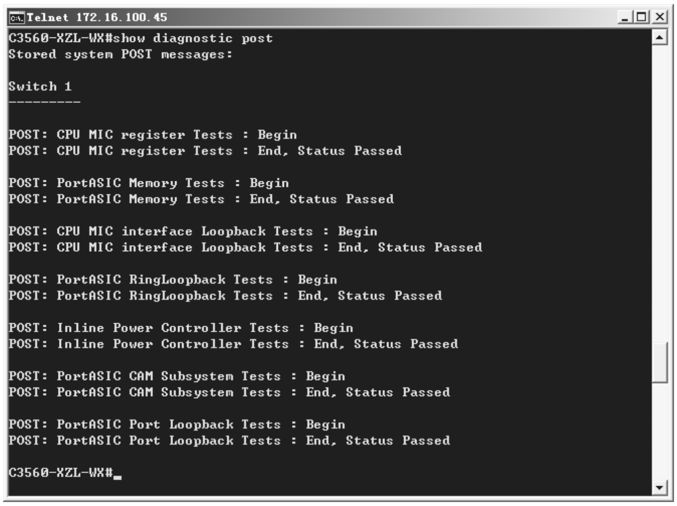


```
C3560-XZL-WX#show diagnostic content

:

  Diagnostics test suite attributes:
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Switch will reload after test list completion / NA
      P/* - will partition stack / NA

                                                        Test Interval   Thre-
  ID   Test Name                          Attributes      day hh:mm:ss.ms shold
  ==== ================================== ============    =============== =====
    1) TestPortAsicStackPortLoopback ---> B*N****I**      not configured  n/a
    2) TestPortAsicLoopback ------------> B*D*X**IR*      not configured  n/a
    3) TestPortAsicCam -----------------> B*D*X**IR*      not configured  n/a
    4) TestPortAsicRingLoopback --------> B*D*X**IR*      not configured  n/a
    5) TestMicRingLoopback -------------> B*D*X**IR*      not configured  n/a
    6) TestPortAsicMem -----------------> B*D*X**IR*      not configured  n/a


C3560-XZL-WX#
```

图 7-2　显示在线诊断测试配置

显示 POST（power-on self-test，加电自检）结果（如图 7-3 所示）。

```
show diagnostic post
```



```
C3560-XZL-WX#show diagnostic post
Stored system POST messages:

Switch 1
---------

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC interface Loopback Tests : Begin
POST: CPU MIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: Inline Power Controller Tests : Begin
POST: Inline Power Controller Tests : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

C3560-XZL-WX#
```

图 7-3　显示 POSE 结果

7.1.2 监控端口模块和状态

1. 检查模块状态

对于多插槽交换机而言，可以使用 show module all 命令检查已经安装的模块，以及每个模块的 MAC 地址、版本号及工作状态。当然，也可以只检查指定的模块。

检查所有模块的状态（如图 7-4 所示）。

```
Switch# show module all
```

```
Telnet 172.16.100.1
C6509-ZX-HX1#show module all
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1   24  CEF720 24 port 1000mb SFP              WS-X6724-SFP       SAL11370F3Q
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAL1133XRYB
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-3B       SAL11370MAW
  7    8  CEF720 8 port 10GE with DFC            WS-X6708-10GE      SAL11391KL7
  9    6  Firewall Module                        WS-SVC-FWM-1       SAD113405Y5

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  0019.3036.fd20 to 0019.3036.fd37   2.6   12.2(14r)S5  12.2(18)SXF1 Ok
  3  001c.58d3.cf90 to 001c.58d3.cfbf  11.3   7.2(1)       8.5(0.46)RFW Ok
  5  001a.2f3c.3e68 to 001a.2f3c.3e6b   5.4   8.4(2)       12.2(18)SXF1 Ok
  7  001a.6c9e.8080 to 001a.6c9e.8087   1.3   12.2(18r)S1  12.2(18)SXF1 Ok
  9  001d.4587.422c to 001d.4587.4233   4.2   7.2(1)       3.2(1)       Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  1  Centralized Forwarding Card WS-F6700-CFC       SAL1135Z75Z  4.0    Ok
  5  Policy Feature Card 3       WS-F6K-PFC3B       SAL11370KCT  2.3    Ok
  5  MSFC3 Daughterboard         WS-SUP720          SAL11370K5A  3.0    Ok
  7  Distributed Forwarding Card WS-F6700-DFC3C     SAL113811YA  1.0    Ok

Mod  Online Diag Status
---- -------------------
  1  Pass
  3  Pass
  5  Pass
  7  Pass
  9  Pass
C6509-ZX-HX1#_
```

图 7-4　检查所有模块的状态

检查指定模块的状态（如图 7-5 所示）。

Switch# **show module** *mod_num*

```
Telnet 172.16.100.1
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#show module 1
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1   24  CEF720 24 port 1000mb SFP              WS-X6724-SFP       SAL11370F3Q

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  0019.3036.fd20 to 0019.3036.fd37   2.6   12.2(14r)S5  12.2(18)SXF1 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  1  Centralized Forwarding Card WS-F6700-CFC       SAL1135Z75Z  4.0    Ok

Mod  Online Diag Status
---- -------------------
  1  Pass
C6509-ZX-HX1#_
```

图 7-5　检查指定模块的状态

当需要查看端口工作状态时，可以使用 show interfaces status 命令（如图 7-6 所示）。

Switch# **show interfaces status**

```
Telnet 172.16.100.1
C6509-ZX-HX1#show interfaces status

Port    Name               Status       Vlan       Duplex  Speed Type
Gi1/1   dongjifang         notconnect   50           full   1000 1000BaseSX
Gi1/2   boshishi           notconnect   1            full   1000 1000BaseLH
Gi1/3   jingguan_techer    connected    46           full   1000 1000BaseLH
Gi1/4                      notconnect   1            full   1000 No Transceiver
Gi1/5                      notconnect   1            full   1000 No Transceiver
Gi1/6                      notconnect   1            full   1000 No Transceiver
Gi1/7                      notconnect   1            full   1000 No Transceiver
Gi1/8                      notconnect   1            full   1000 No Transceiver
Gi1/9                      notconnect   1            full   1000 No Transceiver
Gi1/10                     notconnect   1            full   1000 No Transceiver
Gi1/11                     notconnect   1            full   1000 No Transceiver
Gi1/12                     notconnect   1            full   1000 No Transceiver
Gi1/13                     notconnect   1            full   1000 No Transceiver
Gi1/14                     notconnect   1            full   1000 No Transceiver
Gi1/15                     notconnect   1            full   1000 No Transceiver
Gi1/16                     notconnect   1            full   1000 No Transceiver
Gi1/17                     notconnect   1            full   1000 No Transceiver
Gi1/18                     notconnect   1            full   1000 No Transceiver
Gi1/19                     notconnect   1            full   1000 No Transceiver
Gi1/20                     notconnect   1            full   1000 No Transceiver
Gi1/21                     notconnect   1            full   1000 No Transceiver
 --More-- _
```

图 7-6　查看端口工作状态

2. 检查端口状态

显示所有端口或指定端口的状态和配置（如图 7-7 所示）。

show interfaces [*interface-id*]

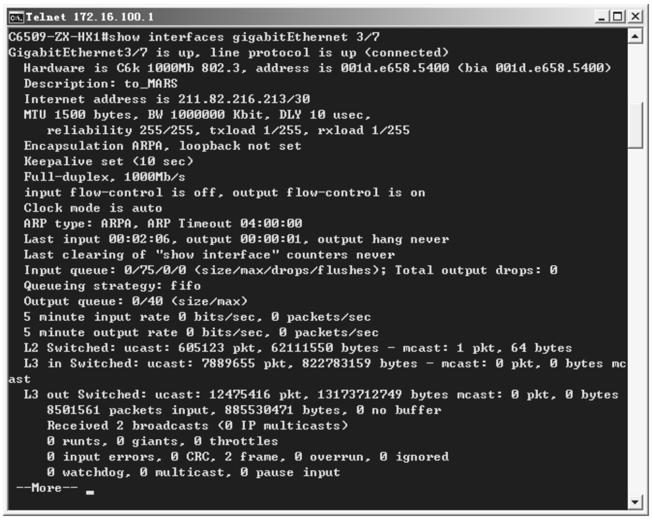

```
Telnet 172.16.100.1
C6509-ZX-HX1#show interfaces gigabitEthernet 3/7
GigabitEthernet3/7 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 001d.e658.5400 (bia 001d.e658.5400)
  Description: to_MARS
  Internet address is 211.82.216.213/30
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is on
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:06, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 605123 pkt, 62111550 bytes - mcast: 1 pkt, 64 bytes
  L3 in Switched: ucast: 7889655 pkt, 822783159 bytes - mcast: 0 pkt, 0 bytes mc
ast
  L3 out Switched: ucast: 12475416 pkt, 13173712749 bytes mcast: 0 pkt, 0 bytes
     8501561 packets input, 885530471 bytes, 0 no buffer
     Received 2 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
 --More--
```

图 7-7　显示端口状态和配置信息

显示接口状态或处于 error-disable 状态的接口列表（如图 7-8 所示）。

show interfaces *interface-id* **status [err-disabled]**

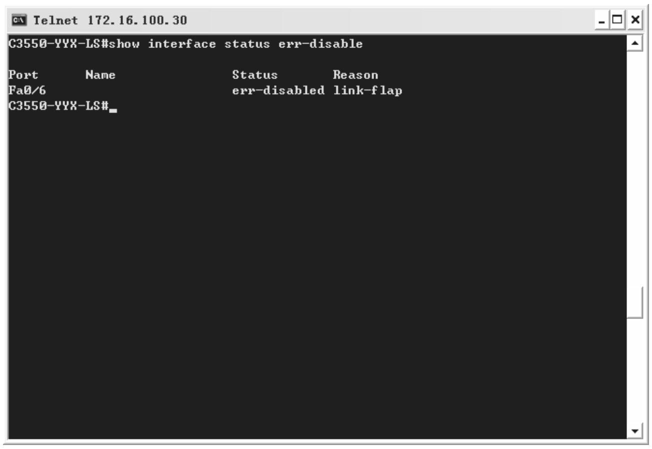

```
Telnet 172.16.100.30
C3550-YYX-LS#show interface status err-disable

Port      Name               Status       Reason
Fa0/6                        err-disabled link-flap
C3550-YYX-LS#
```

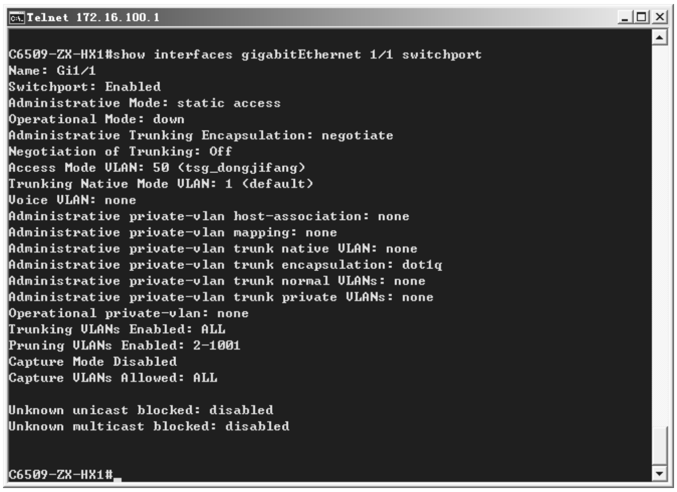
图 7-8　显示处于 error-disable 状态的接口

显示交换端口（非路由端口）的管理或运行状态。可以使用该命令了解指定端口处于交换模式还是路由模式（如图 7-9 所示）。

show interfaces [*interface-id*] **switchport**

显示某个端口或所有端口的描述配置，以及端口状态（如图 7-10 所示）。

show interfaces [*interface-id*] **description**



```
Telnet 172.16.100.1
C6509-ZX-HX1#show interfaces gigabitEthernet 1/1 switchport
Name: Gi1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 50 (tsg_dongjifang)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled


C6509-ZX-HX1#
```

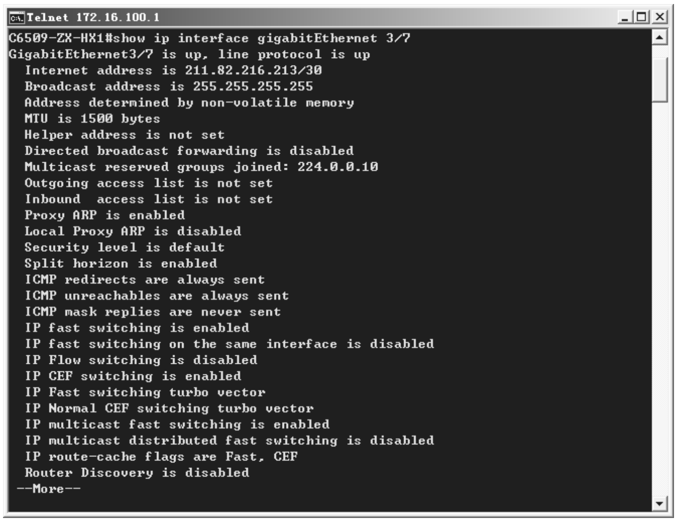
图 7-9　显示交换端口的管理或运行状态

```
Telnet 172.16.100.1
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#show interfaces gigabitEthernet 3/2 description
Interface                      Status         Protocol Description
Gi3/2                          up             up       to_HX-6509-2
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
```

图 7-10　显示端口描述

显示所有或指定的 IP 路由接口配置的可用性状态（如图 7-11 所示）。

show ip interface [*interface-id*]

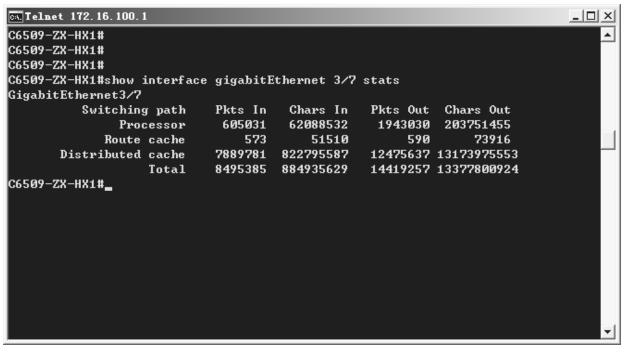


```
Telnet 172.16.100.1
C6509-ZX-HX1#show ip interface gigabitEthernet 3/7
GigabitEthernet3/7 is up, line protocol is up
  Internet address is 211.82.216.213/30
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
 --More--
```

图 7-11　显示 IP 路由接口配置的可用性状态

显示指定接口的输入和输出包（如图 7-12 所示）。

show interface [*interface-id*] stats

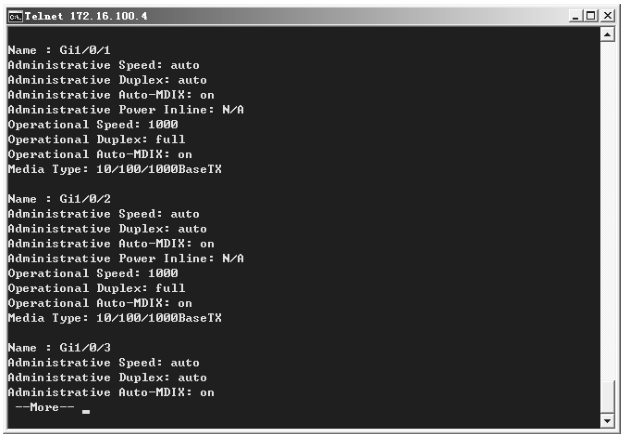


```
Telnet 172.16.100.1
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#show interface gigabitEthernet 3/7 stats
GigabitEthernet3/7
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor     605031   62088532    1943030  203751455
             Route cache        573      51510        590      73916
       Distributed cache    7889781  822795587   12475637 13173975553
                   Total    8495385  884935629   14419257 13377800924
C6509-ZX-HX1#_
```

图 7-12　显示指定接口的输入和输出包

显示接口的速率、双工模式和在线供电设置等属性（如图 7-13 所示）。

show interfaces transceiver *properties*

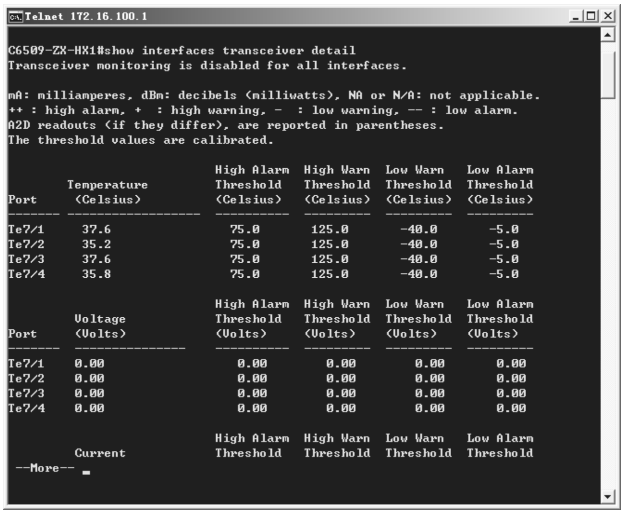


```
Telnet 172.16.100.4

Name : Gi1/0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 1000
Operational Duplex: full
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX

Name : Gi1/0/2
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 1000
Operational Duplex: full
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX

Name : Gi1/0/3
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
 --More-- _
```

图 7-13　显示接口速率等属性

显示接口当前的温度、电压等参数（如图 7-14 所示）。

show interfaces transceiver detail

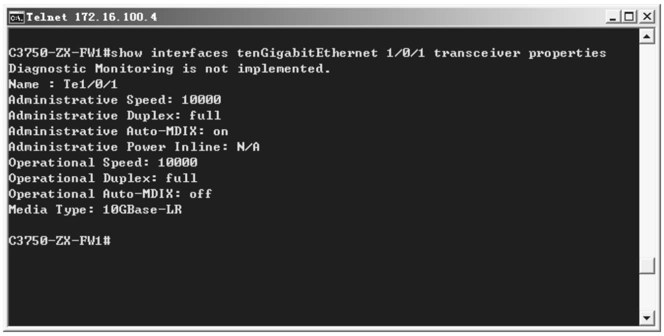


```
Telnet 172.16.100.1

C6509-ZX-HX1#show interfaces transceiver detail
Transceiver monitoring is disabled for all interfaces.

mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

                                    High Alarm  High Warn  Low Warn   Low Alarm
        Temperature                 Threshold   Threshold  Threshold  Threshold
Port     (Celsius)                  (Celsius)   (Celsius)  (Celsius)  (Celsius)
-------  ------------------         ----------  ---------  ---------  ---------
Te7/1      37.6                       75.0       125.0      -40.0       -5.0
Te7/2      35.2                       75.0       125.0      -40.0       -5.0
Te7/3      37.6                       75.0       125.0      -40.0       -5.0
Te7/4      35.8                       75.0       125.0      -40.0       -5.0

                                    High Alarm  High Warn  Low Warn   Low Alarm
         Voltage                    Threshold   Threshold  Threshold  Threshold
Port     (Volts)                    (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------            ----------  ---------  ---------  ---------
Te7/1    0.00                          0.00        0.00       0.00       0.00
Te7/2    0.00                          0.00        0.00       0.00       0.00
Te7/3    0.00                          0.00        0.00       0.00       0.00
Te7/4    0.00                          0.00        0.00       0.00       0.00

                                    High Alarm  High Warn  Low Warn   Low Alarm
         Current                    Threshold   Threshold  Threshold  Threshold
 --More-- _
```

图 7-14　显示接口温度等参数

显示 SFP 模块的物理或运行状态（如图 7-15 所示）。

show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]

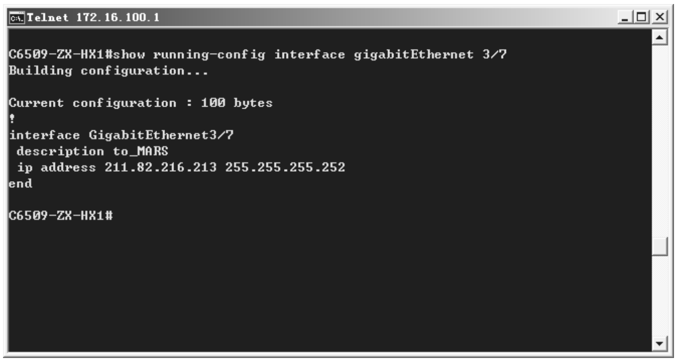


```
C3750-ZX-FW1#show interfaces tenGigabitEthernet 1/0/1 transceiver properties
Diagnostic Monitoring is not implemented.
Name : Te1/0/1
Administrative Speed: 10000
Administrative Duplex: full
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 10000
Operational Duplex: full
Operational Auto-MDIX: off
Media Type: 10GBase-LR

C3750-ZX-FW1#
```

图 7-15　显示 SFP 模块状态

显示接口在 RAM 中的运行配置（如图 7-16 所示）。

show running-config interface [*interface-id*]

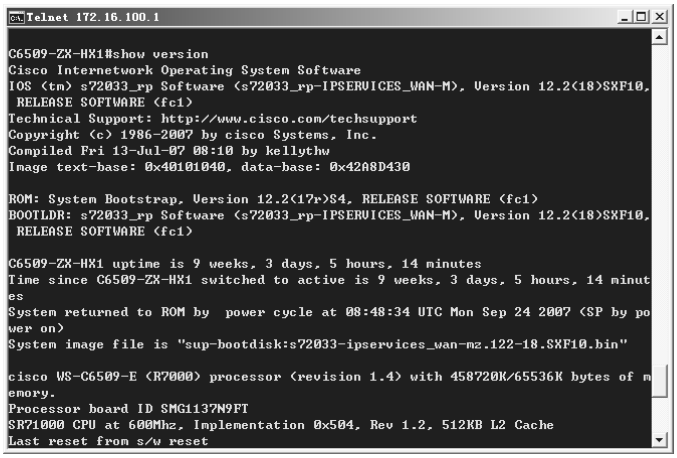


```
C6509-ZX-HX1#show running-config interface gigabitEthernet 3/7
Building configuration...

Current configuration : 100 bytes
!
interface GigabitEthernet3/7
 description to_MARS
 ip address 211.82.216.213 255.255.255.252
end

C6509-ZX-HX1#
```

图 7-16　显示接口运行配置

显示硬件配置、软件版本、名称和配置文件来源，以及引导映像（如图 7-17 所示）。

show version

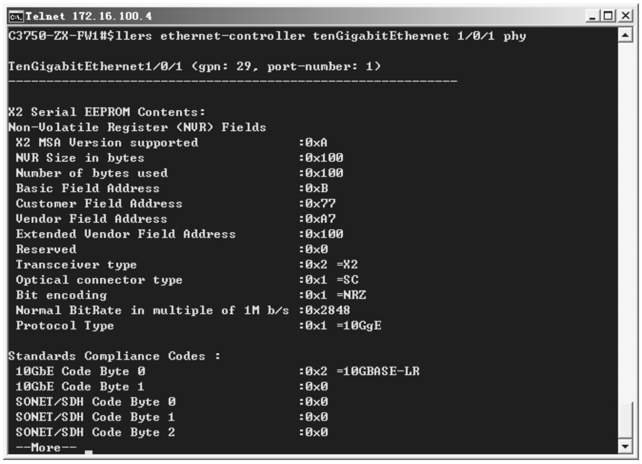


```
C6509-ZX-HX1#show version
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICES_WAN-M), Version 12.2(18)SXF10,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Fri 13-Jul-07 08:10 by kellythw
Image text-base: 0x40101040, data-base: 0x42A8D430

ROM: System Bootstrap, Version 12.2(17r)S4, RELEASE SOFTWARE (fc1)
BOOTLDR: s72033_rp Software (s72033_rp-IPSERVICES_WAN-M), Version 12.2(18)SXF10,
 RELEASE SOFTWARE (fc1)

C6509-ZX-HX1 uptime is 9 weeks, 3 days, 5 hours, 14 minutes
Time since C6509-ZX-HX1 switched to active is 9 weeks, 3 days, 5 hours, 14 minut
es
System returned to ROM by  power cycle at 08:48:34 UTC Mon Sep 24 2007 (SP by po
wer on)
System image file is "sup-bootdisk:s72033-ipservices_wan-mz.122-18.SXF10.bin"

cisco WS-C6509-E (R7000) processor (revision 1.4) with 458720K/65536K bytes of m
emory.
Processor board ID SMG1137N9FT
SR71000 CPU at 600Mhz, Implementation 0x504, Rev 1.2, 512KB L2 Cache
Last reset from s/w reset
```

图 7-17　显示配件配置等信息

显示指定接口 auto-MDIX 功能的操作状态（如图 7-18 所示）。

show controllers ethernet-controller *interface-id* **phy**



```
Telnet 172.16.100.4
C3750-ZX-FW1#$llers ethernet-controller tenGigabitEthernet 1/0/1 phy

TenGigabitEthernet1/0/1 (gpn: 29, port-number: 1)
-----------------------------------------------------------

X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 X2 MSA Version supported             :0xA
 NVR Size in bytes                    :0x100
 Number of bytes used                 :0x100
 Basic Field Address                  :0xB
 Customer Field Address               :0x77
 Vendor Field Address                 :0xA7
 Extended Vendor Field Address        :0x100
 Reserved                             :0x0
 Transceiver type                     :0x2  =X2
 Optical connector type               :0x1  =SC
 Bit encoding                         :0x1  =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type                        :0x1  =10GgE

Standards Compliance Codes :
 10GbE Code Byte 0                    :0x2  =10GBASE-LR
 10GbE Code Byte 1                    :0x0
 SONET/SDH Code Byte 0                :0x0
 SONET/SDH Code Byte 1                :0x0
 SONET/SDH Code Byte 2                :0x0
 --More--
```

图 7-18　显示 auto-MDIX 功能的操作状态

显示交换机或指定接口的 PoE 状态（如图 7-19 所示）。

show power inline [*interface-id*]

```
Telnet 172.16.100.45
C3560-XZL-WX#
C3560-XZL-WX#
C3560-XZL-WX#
C3560-XZL-WX#
C3560-XZL-WX#
C3560-XZL-WX#show power inline FastEthernet0/1
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   on         15.0    AIR-LAP1242AG-C-K9  3     15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa0/1                 15.4                15.4
C3560-XZL-WX#
```

图 7-19　显示 PoE 状态

3. 清除接口计数与复位硬件逻辑

清除接口计数（如图 7-20 所示）。

clear counters [*interface-id*]

```
Telnet 172.16.100.1
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#clear counters tenGigabitEthernet 7/2
Clear "show interface" counters on this interface [confirm]
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
C6509-ZX-HX1#
```

图 7-20　清除接口计数

复位指定接口的硬件逻辑。

```
clear interface interface-id
```

复位异步串行的硬件逻辑。

```
clear line [number | console 0 | vty number]
```

7.1.3 查看MAC地址表

显示指定MAC地址的MAC地址表信息。

```
Switch# show mac-address-table address mac_address
```

显示指定接口的MAC地址表信息。

```
Switch# show mac-address-table interface interface_id
```

7.1.4 TDR线缆测试

当不能建立连接时，使用TDR（Time Domain Reflectometer时域反射器）可以测试线缆。该测试在更换现有交换机、升级至千兆位或万兆位以太网、或安装新的电缆插件后，显得更为重要。

① 开始TDR测试。

```
Switch# test cable-diagnostics tdr {interface interface_id}
```

② 显示TDR测试内容信息。

```
Switch# show cable-diagnostics tdr {interface interface_id }
```

7.2 管理交换机

7.2.1 TFTP服务器

TFTP（Trivial File Transfer Protocol）服务器可实现交换机或交换机软件系统的保存和升级、配置文件的保存和下载，使得对交换机和交换机的管理变得简单和快捷。因此，在进行交换机和交换机的管理前，应先安装一台Cisco TFTP服务器。TFTP服务器软件可在Cisco网站（http://www.cisco.com/）下载。

任何一台计算机只要安装有FTFP服务器软件，即可成为TFTP服务器。软件安装完毕，即可将下载的Cisco Catalyst系统软件映像复制到该TFTP服务器根目录下（C:\Program Files\Cisco Systems\Cisco TFTP Server），并通过该TFTP服务器实现交换机或交换机软件的升级，以及配置文件的备份与恢复。运行Cisco TFTP Server，显示如图7-21所示的主窗口界面。

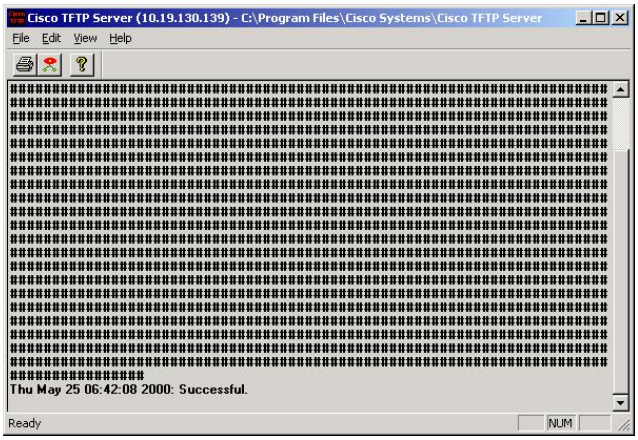


图 7-21　Cisco TFTP Server 主窗口界面

7.2.2 系统文件管理

1. 显示和管理文件

在操作之前，可以先查看文件系统内容列表。例如，在复制新的配置文件到 Flash 内存时，可以先查看文件系统是否有足够的空间，以及是否有同名文件。

■ **查看文件**

在特权模式下使用命令，可以显示交换机上可用的文件系统。表 7-1 所示为文件系统字段描述。

```
Switch# show file systems
```

表 7-1　文件系统字段描述

字　段	值
Size(b)	文件系统中内存的大小，单位为 byte
Free(b)	文件系统中空闲内存的大小，单位为 byte
Type	文件系统类型 flash—Flash 内存设备 nvram—NVRAM 设备 opaque—本地生成的 pseudo 文件系统或下载接口 unknown—未知类型
Flags	文件系统权限 ro—只读 rw—读/写 wo—只写
Prefixes	文件系统别名 flash—Flash 文件系统 nvram—NVRAM null—Null（空），可以将远程文件复制至 Null 以查看其大小 rcp— RCP（Remote Copy Protocol，远程复制协议）网络服务器 system—系统内存容量，包括运行配置（running configuration） tftp—TFTP 网络服务器 xmodem—使用 Xmodem 协议从网络计算机中获得文件 ymodem—使用 Ymodem 协议从网络计算机中获得文件

显示文件系统中的文件列表。

```
dir [/all] [filesystem:][filename]
```

查看文件系统中有关每个文件的更多信息。

```
show file systems
```

显示指定文件的信息。

```
show file information file-url
```

显示打开文件列表描述。

```
show file descriptors
```

■ **复制文件**

复制文件。

```
copy source-url destination-url
```

源和目的URL可以使用running-config和startup-config关键字，例如，copy running-config startup-config命令可以将当前运行配置保存至NVRAM中，以便在下次系统初始化时使用。

也可以像文件系统中的文件一样，从远程计算机使用Xmodem或Ymodem协议复制指定文件系统（xmodem:, ymodem:）中的文件。

网络文件系统URL包括ftp:、rcp:和tftp:，语法如下。

- FTP——ftp:[[*//username* [:*password*]@*location*]/*directory*]/*filename*
- RCP——rcp:[[*//username@location*]/*directory*]/*filename*
- TFTP——tftp:[[*//location*]/*directory*]/*filename*

本地可写文件系统包括flash:。

也有一些无效的源和目的组合。特别是，不能复制以下组合。

- 从一个运行配置（running configuration）到一个运行配置
- 从一个开始配置（startup configuration）到一个开始配置
- 从一个设备到同一设备（例如，copy flash: flash:命令是无效的）

■ **删除文件**

当不再需要Flash中的文件时，可以考虑将其删除。使用如下命令，可以从指定Flash设备中删除指定的文件或目录。

```
delete [/force] [/recursive] [filesystem:]/file-url
```

当尝试删除任何文件时，系统都将提示用户确认删除操作。使用/recursive关键字，将删除该目录，以及包含其中的所有子目录和文件。使用/force关键字，将在删除每个文件或子目录时不再显示警告提示。

> **注意** 文件被删除后，其内容不可恢复。

2. 显示和管理目录

列出指定文件系统中的目录结构。

```
dir filesystem:
```

改变至感兴趣的目录。

```
cd new_configs
```

显示工作目录。

```
pwd
```

创建新目录。目录名称最多允许 45 个字符，且不能包括控制符号、空格、斜线、分号和冒号等字符。

```
mkdir new_configs
```

删除目录。使用 delete /force /recursive *filesystem:/file-url* 命令，可以删除目录中所有的文件和子目录。

```
delete old_configs
```

7.2.3 配置文件管理

1. 恢复出厂默认设置

■ **复位交换机配置**

在将交换机恢复至出厂默认值前，应当先备份交换机的配置。基于 Cisco IOS 的交换机分别拥有一个运行配置（running configuration）文件和启动配置（startup configuration）文件。RAM 中存储运行配置，NVRAM 中存储启动配置。当修改运行 Cisco IOS 系统的交换机的配置时，只是在部分修改运行配置。必须将修改的配置保存至启动配置，否则，在交换机重新装载或重新加电时，修改的配置将会丢失。原因很简单，运行配置只被保存于 RAM 中，而 RAM 中的数据在重新装载或回电时即丢失。若欲将运行配置保存至 NVRAM 中，可以使用 write memory 命令或 copy running-config startup-config 命令。如果没有将修改保存至 NVRAM，那么，在交换机重新加载时，配置的修改部分将从 RAM 中清除。

运行 Cisco IOS 的 Catalyst 模块或固定配置交换机，有独立的文件存储 VLAN 信息，文件名为 vlan.dat，模块化交换机存储在 NVRAM 中，固定配置交换机存储在 Flash 中。若欲将交换机复位至出厂默认值，需要删除启动配置和 vlan.dat 文件。

若欲复位交换机至出厂默认值，使用 erase startup-config 或 write erase 命令。这些命令不能清除引导变量，如配置寄存器（config-register）和引导系统设置。可以使用 boot 命令修改引导系统参数。在运行 Cisco IOS 软件的 Catalyst 4900/4500 和 6800/6500 交换机中，可以使用 config-register 命令修改配置寄存器值。

如下所示为使用 write erase 命令将 Catalyst 2960 交换机恢复至出厂默认配置。较早版本的 Catalyst 4500/4000 和 Catalyst 6500/6000 系列交换机，Catalyst 2940、Catalyst 2950/2955、Catalyst

2970、Catalyst 3550、Catalyst 3560、Catalyst 3750 系列交换机的操作与之相同。

```
Cat2960# write erase
Erasing the nvram filesystem will remove all files! Continue? [confirm]y[OK]
Erase of nvram: complete
Cat2960#
Cat2960# reload
System configuration has been modified. Save? [yes/no]: n
!--- Do not save the configuration at this prompt. Otherwise, the switch
!--- reloads with the current running configuration and does not reset to default.
Proceed with reload? [confirm]y
2w0d: %SYS-5-RELOAD: Reload requested
C2960 Boot Loader (C2960-HBOOT-M) Version 13.2(11r)EA1, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-12 12:58 by antonino
WS-C2960-12-EI starting...
…
Press RETURN to get started!
00:00:37: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
00:00:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
Switch>
```

对于 Catalyst 3850/3650/3750-X/3560-X/2960-X 系列固定配置交换机而言，可以采用如下操作将交换机恢复至出厂默认配置。

① 如果交换机采用 Cisco IOS XE Release 3.6.0E 或更新版本，键入 erase startup-config 特权配置命令可以清除启动配置。如果使用较早版本，则可以跳过该步骤。

② 按下并按住 Mode 按钮，交换机 LED 指示灯在 3 秒钟后开始闪烁。

③ 继续按住 Mode 按钮，LED 指示灯在 7 秒钟后停止闪烁，交换机开始重新启动。

④ 重新启动后，交换机配置被清除。

较新版本的 Catalyst 4900/4500 系列交换机可以使用 erase /all non-default 命令，清除管理引擎中（NVRAM 和 Flash）的永久配置和状态，并将交换机设置为出厂默认状态。

```
Switch# erase /all non-default
Erase and format operation will destroy all data in non-volatile storage.
Continue? [confirm]
Formatting bootflash: ...
Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
 ConfigReg=0x2101
 PS1=rommon ! >
 EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

如果 Catalyst 4900/4500 系列交换机可以连接到 TFTP 服务器，可以使用 copy 命令将映像文件拷贝到 bootflash 内存。

```
Switch# copy tftp://tftp_server_IP_address/img_dir/ cat4500-entservices-mz.bin bootflash:
```

拷贝完成后，可以使用 reload 命令重新引导交换机。

```
Switch# reload
 System configuration has been modified. Save? [yes/no]: no
 Proceed with reload? [confirm]
00:06:17: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

■ **复位 VLAN 信息**

将 VLAN 信息复位至出厂默认值，应当从 Flash 或 NVRAM 中删除 vlan.dat，并重新引导交换机。在运行 Cisco IOS 软件的 Catalyst 6800/6500/6000 系列交换机上，vlan.dat 文件存储在 const_nvram 中。在运行 Cisco IOS 软件的 Catalyst 4900/4500/4000 系列交换机上，vlan.dat 存储在 cat4000_flash:中。在 Catalyst 2950/2960/3550/3560/3650/3750/3850 固定配置交换机上，vlan.dat 存储于 flash:中。

如下示例中显示了如何在 Catalyst 固定配置交换机中删除 VLAN 信息，可以使用相同的步骤删除 Catalyst 6500/6000 和 4500/4000 中的 VLAN 信息。

① 查看 Flash 或 NVRAM 中的 VLAN 信息。

```
Cat2960# show vlan
```

② 校验 vlan.dat 文件所在的位置。Catalyst 4500/4000 交换机使用 dir cat 4000_flash:命令，Catalyst 6500/6000 交换机使用 dir const_nvram 命令。

```
Cat2960# dir flash:
```

③ 删除 VLAN 信息，重新引导交换机。

```
Cat2960# delete flash:vlan.dat
Delete filename [vlan.dat]?
!--- 按下 Enter 键
Delete flash:vlan.dat? [confirm]y
Cat2960# reload
```

提·示 在运行较早版本 Cisco IOS 软件的 Catalyst 6500/6000 和 4500/4000 交换机上，delete 命令可能不工作。作为替代，必须使用 erase const_nvram: 或 erase cat4000_flash:命令。不能在语法中指定 vlan.dat 文件。然而，在较近版本的 Cisco IOS 中，Catalyst 6500/6000 可以使用 delete const_nvram:vlan.dat 命令，Catalyst 4500/4000 可以使用 delete cat4000_flash:vlan.dat 命令。

2. 配置文件的备份

交换机的配置文件也可以像普通计算机一样进行复制。但是，与普通计算机不同之处在

于，无论是上传还是下载文件，都必须在操作终端上安装 TFTP 软件，将其配置成为 TFTP 服务器，借助 TFTP 服务器实现对配置文件的操作。

> **提·示** 上传配置文件，不仅可以快速恢复原有交换机的配置，而且还可以作简单修改后，用于快速配置其他交换机。主要修改内容包括：管理 IP 地址、VLAN 设置和其他端口设置。由于配置文件是文本文件，可以使用记事本或写字板打开编辑，并使用"查找"、"替换"的方式快速更换批量修改，准确而高效。

■ **准备工作**

可以配置文件上传至 TFTP 服务器实现交换机配置文件的备份。在将配置文件上传至 TFTP 服务器之前，确认已经完成以下工作。

- 确认已经安装了一台 TFTP 服务器。
- 确认交换机能够与 TFTP 服务器正常通信，交换机和路由器必须位于同一子网。
- 在上传映像之前，可能需要在 TFTP 服务器上创建一个空的文件。
- 如果覆盖一个已经存在的文件（包括空文件，如果已经创建了的话），确认赋予了相应的权限，即赋予其 world-write 权限。

■ **备份配置文件**

① 将配置文件复制至 TFTP 服务器的适当文件夹。默认安装文件夹为"C:\Program Files\Cisco Systems\Cisco TFTP Server"。

② 通过 Console 端口或 Telnet 登录至交换机。

③ 使用 copy 命令，将配置文件下载到 TFTP 服务器。

把当前启动配置复制至 TFTP 服务器，备份启动配置文件。

```
copy startup-config tftp
```

把当前运行配置复制至 TFTP 服务器，备份当前运行配置。

```
copy running-config tftp
```

操作过程如图 7-22 所示。

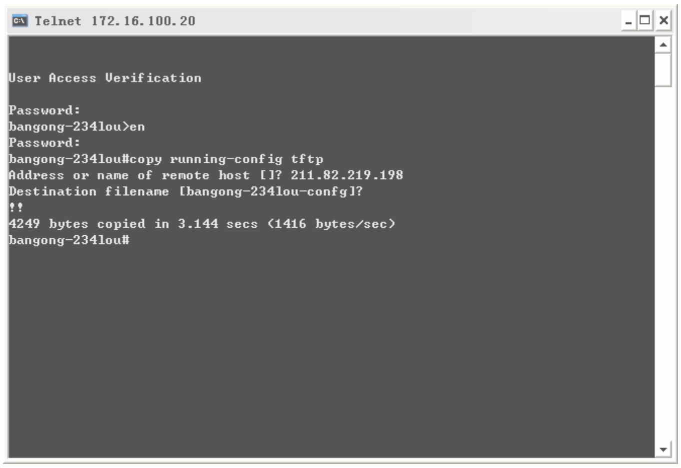


图 7-22　备份配置文件操作过程

3. 配置文件的恢复

■ **准备工作**

在从 TFTP 服务器下载配置文件前，确认已经完成以下工作。

- 确认已经安装了一台 TFTP 服务器。
- 确认交换机能够与 TFTP 服务器正常通信。
- 确认配置文件被下载至服务器的适当目录。
- 确认文件被设置了 world-read 权限。

■ **恢复配置文件**

① 根据需要修改交换机配置文件，并将配置文件复制至 TFTP 服务器的适当文件夹。默认安装文件夹为“C:\Program Files\Cisco Systems\Cisco TFTP Server”。

② 通过 Console 端口或 Telnet 登录至交换机。

③ 使用 **copy** 命令，从 TFTP 服务器下载配置文件。在提示符下，指定 TFTP 服务器的 IP 地址或主机名，以及目的文件名，配置文件将被上传至 TFTP 服务器。

把配置文件从 TFTP 服务器复制至 NVRAM，恢复启动配置文件。

```
copy tftp startup-config
```

把配置文件从 TFTP 服务器复制为当前运行配置，恢复系统配置。

```
copy tftp running-config
```

把当前配置保存至 NVRAM 作为启动配置。

```
copy running-config startup-config
```

随后，交换机即以新的配置文件运行。

7.2.4 IOS 软件映像管理

1. 备份 IOS 软件映像

■ **准备工作**

在将软件映像上传至 TFTP 服务器之前，确认已经完成以下工作。

- 确认已经安装了一台 TFTP 服务器。
- 确认交换机能够与 TFTP 服务器正常通信。
- 在上传映像之前，可能需要在 TFTP 服务器上创建一个空的文件。
- 如果覆盖一个已经存在的文件（包括空文件，如果已经创建了的话），确认赋予了其相应的权限，即赋予其 world-write 权限。

■ **使用 TFTP 服务器上传软件映像**

① 通过 Console 端口或 Telnet 登录至交换机。

② 使用“**copy flash tftp**”命令，将软件映像上传至 TFTP 服务器。在提示符下，指定 TFTP 服务器地址和目的文件名。系统映像将被上传至 TFTP 服务器。

2. 恢复系统软件映像

使用 TFTP 服务器，可以通过网络将系统软件映像下载到交换机。当软件映像下载时，该映像文件被下载至超级引擎 Flash 内存中。在 Flash 内存中可以保存多个映像文件。

■ 准备工作

在使用 TFTP 下载软件系统映像前，确认已经完成下述工作。

- 确认已经安装了一台 TFTP 服务器。
- 确认交换机能够与 TFTP 服务器正常通信。
- 确认软件映像被下载至 TFTP 服务器适当的目录中。
- 确认文件的访问许可设置正确。
- 确认提供了不间断电源。

■ 使用 TFTP 下载超级引擎映像

① 将软件映像复制至 TFTP 服务器适当的目录。

② 通过 Console 端口或 Telnet 登录至交换机。如果使用 Telnet 登录交换机，那么当交换机运行新软件而重新启动时，将断开连接。

③ 使用“**copy tftp flash**”命令从 TFTP 服务器下载软件映像。在提示符下键入 TFTP 服务器的 IP 地址或主机名，以及下载的文件名。交换机将从 TFTP 服务器下载映像文件，并将映像复制至引导闪存。

④ 使用“**reset system**”命令重新启动交换机。如果使用 Telnet 连接至交换机，那么，该 Telnet 进程将断开连接。

⑤ 当交换机重新引导后，键入“**show version**”命令检查交换机上的编码版本。

3. 升级系统软件映像

■ 准备工作

在使用 TFTP 升级软件系统映像前，确认已经完成下述工作。

- 确认已经安装了一台 TFTP 服务器。
- 确认交换机能够与 TFTP 服务器正常通信。
- 确认选择并下载了合适的 Cisco IOS 软件映像。
- 确认软件映像被复制至 TFTP 服务器适当的目录中。
- 确认已经备份了原来的 Cisco IOS 系统映像文件。
- 确认交换机 Flash 容量能够存储新的 Cisco IOS 系统映像。
- 确认 TFTP 服务器和交换机连接至 UPS 稳定电源。

■ Cisco IOS 系统软件升级

下面，以 Catalyst 3550 交换机为例，介绍一下如何将其软件版本由 Cisco IOS Software Release 12.1(12c)EA1 升级至 Cisco IOS Software Release 12.1(13)EA1。新版本的 Cisco IOS 映像软件名称为 c3550-i5q3l2-mz.121-13.EA1.bin，容量为 3 993 612 B，约 4 MB。

① 使用 show version 命令，查看当前软件版本。

```
3550# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(12c)EA1, RELEASE
SOFTWARE (fc1)
```

② 使用 dir flash:命令，查看 Flash 中的文件，以及可用内存。

```
3550# dir flash:
Directory of flash:/
  2 -rwx      556   Mar 01 1993 00:02:13 vlan.dat
  3 -rwx  3384393   Mar 01 2009 00:32:58 c3550-i5q3l2-mz.121-9.EA1c.bin
  4 drwx      192   Mar 01 1993 00:10:15 c3550-i5q3l2-mz.121-11.EA1a
 38 -rwx        0   Mar 01 2009 00:10:15 env_vars
  7 -rwx      348   Mar 01 2009 00:10:15 system_env_vars
 12 drwx      192   Mar 01 2009 00:16:22 c3550-i5q3l2-mz.121-12c.EA1
15998976 bytes total (1949184 bytes free)
!--- 内存的自由空间只有不到 2M，显然不够升级新系统软件所需，因此，必须删除旧的系统软件。
其中，属性中标识有“d”的文件为原来已经删除的系统软件。
3550#
```

③ 使用 delete flash:或 delete /force /recursive flash:命令，删除老版本的 Cisco IOS 系统映像。

```
3550# delete flash:c3550-i5q3l2-mz.121-9.EA1c.bin
Delete filename [c3550-i5q3l2-mz.121-9.EA1c.bin]?

!--- 回车确认

Delete flash:c3550-i5q3l2-mz.121-9.EA1c.bin? [confirm]

!--- 回车确认

3550#
3550# dir flash:
Directory of flash:/
  2 -rwx      556   Mar 01 1993 00:02:13 vlan.dat
  4 drwx      192   Mar 01 1993 00:10:15 c3550-i5q3l2-mz.121-11.EA1a
 38 -rwx        0   Mar 01 1993 00:10:15 env_vars
  7 -rwx      348   Mar 01 1993 00:10:15 system_env_vars
 12 drwx      192   Mar 01 1993 00:16:22 c3550-i5q3l2-mz.121-12c.EA1
15998976 bytes total (5334016 bytes free)
!--- 删除旧的 Cisco IOS 映像文件之后，已经有 5 MB 的自由空间，完全满足升级软件所需
```

或者

```
3550# delete /force /recursive flash:c3550-i5q3l2-mz.121-11.EA1a
Delete filename [c3550-i5q3l2-mz.121-11.EA1a]?
!--- 回车确认删除
3550#
```

```
3550# dir flash:
Directory of flash:/
   2  -rwx        556   Mar 01 1993 00:02:13  vlan.dat
  38  -rwx          0   Mar 01 1993 00:10:15  env_vars
   7  -rwx        348   Mar 01 1993 00:10:15  system_env_vars
  12  drwx        192   Mar 01 1993 00:16:22  c3550-i5q3l2-mz.121-12c.EA1
15998976 bytes total (10417664 bytes free)
!--- 已经拥有了 10 MB 自由空间

3550#
```

④ 使用 copy tftp flash:命令，将新版本的 Cisco IOS 系统映像复制至 Flash。

```
3550# copy tftp flash:
Address or name of remote host []? 192.167.100.100

!--- 192.167.100.100 是 TFTP 服务器的 IP 地址。回车确认。

Source filename []? c3550-i5q3l2-mz.121-13.EA1.bin

!--- 回车确认。

Destination filename [c3550-i5q3l2-mz.121-13.EA1.bin]?
Accessing tftp://20.20.20.2/c3550-i5q3l2-mz.121-13.EA1.bin...
Loading     c3550-i5q3l2-mz.121-13.EA1.bin     from     20.20.20.2     (via
Vlan1): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3993612 bytes]

!--- 系统映像复制完成

3993612 bytes copied in 107.992 secs (36981 bytes/sec)
3550# dir flash:
Directory of flash:/
   2  -rwx        556   Mar 01 1993 00:02:13  vlan.dat
   3  -rwx    3993612   Mar 01 1993 01:11:07  c3550-i5q3l2-mz.121-13.EA1.bin

!--- 新的系统映像安装到 flash:目录

  38  -rwx          0   Mar 01 1993 00:10:15  env_vars
   7  -rwx        348   Mar 01 1993 00:10:15  system_env_vars
  12  drwx        192   Mar 01 1993 00:16:22  c3550-i5q3l2-mz.121-12c.EA1
15998976 bytes total (6423552 bytes free)
3550#
```

⑤ 使用 verify flash:命令，校验新复制的 Cisco IOS 系统映像。

```
3550# verify flash:c3550-i5q3l2-mz.121-13.EA1.bin
Verified flash:c3550-i5q3l2-mz.121-13.EA1.bin
3550#
```

```
!--- 校验系统映像文件是否完整无误
```

⑥ 使用 boot system flash: :命令，配置系统引导声明，在下次引导时使用新的系统映像。

```
3550# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3550(config)# boot system flash:c3550-i5q3l2-mz.121-13.EA1.bin
3550(config)# end
3550#
3550# show boot
BOOT path-list:      flash:c3550-i5q3l2-mz.121-13.EA1.bin

!--- 指定引导所使用的系统映像，在下次引导时，以新的系统映像文件引导系统
```

⑦ 保存现有配置，并重新引导系统。

```
3550# write memory
Building configuration...
[OK]
3550# reload
Proceed with reload? [confirm]

!--- 回车确认
```

⑧ 校验 Cisco IOS 系统映像版本。

```
3550# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(13)EA1, RELEASE SOFTWARE
(fc1)
```

7.3 配置网络远程管理

7.3.1 配置 CDP

使用 CDP（Cisco Discovery Protocol）可发现网络中相邻的 Cisco 设备，包括交换机、网桥、访问服务器和交换机，从而便于发现网络的拓扑结构，并实现对所有网络设备的配置和管理。

1. CDP 概述

CDP 是一个可运行于所有 Cisco 产品的网络协议。借助 CDP，可以查看直接连接至该交换机的所有 Cisco 设备。CDP 运行于 OSI 模型的第二层即数据链路层之上，支持任何介质，并支持 SNAP（Subnetwork Access Protocol）。Cisco 设备不转发 CDP 包。当接收到新的 CDP 信息时，旧的信息将被丢弃。

CDP 基本上是用来获取相邻设备的协议地址，以及发现这些设备的平台的。CDP 也可为路由器的使用提供相关接口信息。CDP 是一种独立媒体协议，运行在所有 Cisco 制造的设备上，包括路由器、网桥、接入服务器和交换机。

SNAP 中结合使用 CDP 管理信息基础 MIB，能使网络管理应用获知设备类型和相邻设备的SNMP代理地址，并向这些设备发送SAMP查询请求。Cisco发现协议支持CISCO-CDP-MIB。

CDP 运行在所有的媒体上，从而支持子网访问协议 SNAP，包括局域网、帧中继和异步传输模式 ATM 物理媒体。CDP 只运行于数据链路层，因此支持不同网络层协议的两个系统彼此相互了解。

CDP 配置每台设备发送周期性信息，即广告到组播地址。每台设备至少广告一个地址，在该地址下，可以接收 SNAP 信息。广告包括生存期，或保持时间等信息，这些信息指出了在取消之前接收设备应该保持 CDP 信息的时间长短。此外每台设备还要注意其他设备发出的周期性 CDP 信息，从中了解相邻设备信息并决定哪些设备的媒体接口什么时候增长或降低。

CDP 版本 2 是目前该协议使用最普遍的版本，具有更高的智能设备跟踪等性能。支持该性能的报告机制，提供快速差错跟踪功能，有利于缩短停机时间（Downtime）。报告差错信息可以发送到控制台或日志服务器（Logging Server），这些差错信息包括连接端口上不匹配（Unmatching）的本地 VLAN IDs（IEEE 802.1q），以及连接设备间不匹配的端口双向状态。

2. CDP 默认配置

CDP 默认配置如表 7-2 所示。

表 7-2　CDP 默认配置

功　　能	默 认 值
CDP 全局状态	启用
CDP 接口状态	所有端口全部启用
CDP 定时器（包更新频率）	60 s
CDP 保留时间（丢弃之前）	180 s
CDP 版本 2 广告	启用

```
CDP timer (packet update frequency)
CDP holdtime (before discarding)
CDP Version-2 advertisements
```

3. 禁用或启用 CDP

借助以下操作，可以在交换机上启用或禁用 CDP 协议。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 启用 CDP。使用 no 命令可以禁用 CDP。

```
Switch(config)# [no] cdp run
```

③ 返回特权配置模式。

```
Switch(config)# end
```

④ 校验配置。

```
Switch# show cdp
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

4. 在接口启用或禁用 CDP

借助以下操作，可以在交换机指定接口上启用或禁用 CDP 协议。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定欲配置的接口，进入接口配置模式。

```
Switch(config)# interface interface-id
```

③ 启用 CDP。使用 no 命令可以禁用 CDP。

```
Switch(config-if)# [no] cdp enable
```

④ 返回特权配置模式。

```
Switch(config)# end
```

⑤ 校验配置。

```
Switch# show cdp interface interface-id
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

5. 配置 CDP 参数

借助以下操作，可以在交换机上配置 CDP 协议参数。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 设置 CDP 更新发送频率。取值范围为 5～254，默认为 60 s。由于 CDP 广告会在某种程度上占用网络带宽，特别是网络中的设备较多时。因此，如果网络拓扑结构相对稳定，那么不妨将更新发送频率设置得低一些。

```
Switch(config)# cdp timer seconds
```

③ 设置保留其他设备发送信息的时间。取值范围为 10～255，默认为 180 s。如果网络拓扑结构相对稳定，那么可以将保留时间设置得长一些。

```
Switch(config)# cdp holdtime seconds
```

④ 设置采用版本 2 发送通告。该状态为默认值。

```
Switch(config)# cdp advertise-v2
```

⑤ 返回特权配置模式。

```
Switch# end
```

⑥ 校验配置。

```
Switch# show cdp
```

⑦ 保存当前配置。

```
Switch# copy running-config startup-config
```

7.3.2 配置 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议），是一个标准的用于管理 IP 网络上结点的协议。SNMP 由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。该协议能够支持网络管理系统，提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理工作站报告问题和错误提供了一种方法。

1. SNMP 简介

SNMP 是应用层协议，是 TCP/IP 协议簇的一部分，是一个从网络上的设备收集管理信息的公用通信协议。SNMP 是管理进程（NMS）和代理进程（Agent）之间的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。通过将 SNMP 嵌入数据通信设备，如路由器、交换机或防火墙中，就可以从一个网管工作站管理这些设备，查询设备信息、修改设备的参数值、监控设备状态、自动发现网络故障、生成报告等，并以图形方式查看信息。

■ SNMP 组成

使用 SNMP 进行网络管理需要几个重要部分，即管理信息库（Management Information Base，MIB）、管理代理（Agent）和网络管理系统（Network Management System，NMS）。

① 管理信息库

管理信息库是对象的集合，它代表网络中可以管理的资源和设备。任何一个被管理的资源都表示成一个对象，称为被管理的对象。定义了被管理对象的一系列属性：对象的名称、对象的访问权限和对象的数据类型等。每个 Agent 都有自己的 MIB。MIB 也可以看作是 NMS 和 Agent 之间的一个接口，通过这个接口，NMS 可以对 Agent 中的每一个被管理对象进行读/写操作，从而达到管理和监控设备的目的。

由于 MIB 有公共的格式，因此，可以借助 SNMP 管理工具收集 MIB 信息，并在管理控制台上呈现给网络管理员。从管理者的角度看，所有的网络管理操作都通过对 MIB 对象的读写、创建和删除完成。MIB 由节点上的 SNMP 代理负责维护，SNMP 代理使用 SNMP 网络管理协议与管理者进行信息交互，把来自管理者的命令或请求转换为本设备特有的指令，完成管理者的指示，并对 MIB 对象进行相应的修改。

② 管理代理

管理代理是一种网络设备的应用模块，服务器、交换机、路由器、无线接入点、网络防火墙等每一个被管理的设备有一个管理代理，用于维护被管理设备的信息数据并响应 NMS 的请求，把管理数据汇报给发送请求的 NMS。Agent 接收到 NMS 的请求信息后，完成查询或修

改操作，并把操作结果发送给 NMS，完成响应。同时，当设备发生故障或者其他事件的时候，Agent 会主动发送陷阱信息给 NMS，通知设备当前的状态变化。

③ 网络管理系统

网络管理系统是网络中的管理者，是一个利用 SNMP 协议对网络设备进行管理和监视的系统，它使用 SNMP 协议发出管理操作的指令，并接受来自 SNMP 代理的通知。NMS 既可以指一台专门用来进行网络管理的服务器，也可以指某个设备中执行管理功能的一个应用程序。

NMS 的基本功能是取得、设置和接收代理发送的意外信息。取得，是指 NMS 发送请求，代理根据这个请求回送相应的数据。设置，是指 NMS 设置管理对象（也就是代理）的值。接收，是指代理可以在 NMS 未请求的状态下，接收代理发送的意外信息，向 NMS 报告发生的意外情况。也就是说，NMS 既可以主动向代理发出请求，查询或修改一个或多个具体的参数值。同时，NMS 可以被动接收代理主动发送的陷阱信息，以获知被管理设备当前的状态。

■ **SNMP 版本**

SNMP 主要有 SNMPv1、SNMPV2c、SNMPv3 几种最常用的版本。

① SNMPv1

SNMPv1 是 SNMP 协议的最初版本，提供最小限度的网络管理功能。SNMPv1 的 SMI 和 MIB 都比较简单，且存在较多安全缺陷。

SNMPv1 采用团体名认证。团体名的作用类似于密码，用来限制 NMS 对 Agent 的访问。如果 SNMP 报文携带的团体名没有得到 NMS/Agent 的认可，该报文将被丢弃。

② SNMPv2c

SNMPv2c 也采用团体名认证。在兼容 SNMPv1 的同时又扩充了 SNMPv1 的功能：它提供了更多的操作类型（GetBulk 操作等）；支持更多的数据类型（Counter32 等）；提供了更丰富的错误代码，能够更细致地区分错误。

③ SNMPv3

SNMPv3 主要在安全性方面进行了增强，它采用了 USM 和 VACM 技术。USM 提供了认证和加密功能，VACM 确定用户是否允许访问特定的 MIB 对象以及访问方式。

USM（基于用户的安全模型）。USM 引入了用户名和组的概念，可以设置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间传输的报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 NMS 和 Agent 之间的通信提供更高的安全性。

VACM（基于视图的访问控制模型）。VACM 技术定义了组、安全等级、上下文、MIB 视图、访问策略五个元素，这些元素同时决定用户是否具有访问的权限，只有具有了访问权限的用户才能管理操作对象。在同一个 SNMP 实体上可以定义不同的组，组与 MIB 视图绑定，组内又可以定义多个用户。当使用某个用户名进行访问的时候，只能访问对应的 MIB 视图定义的对象。

■ **SNMP 操作**

SNMP 支持多种操作，主要为以下几种基本操作：

① get-request　从指定的变量中获取一个值。

② get-next-request　从表内指定的变量中获取一个值。借助该操作，NMS 无需知晓准确的变量名称，而是按顺序在表内查找需要的变量。

③ get-bulk-request　获取大块数据，如表内的多行数据，而不是传输许多小块数据。该命令只由 SNMPv2 及后续版本提供。

④ get-response　对 NMS 发送的 get-request、get-next-request 和 set-request 做出答复

⑤ set-request　将一个值存储至指定变量。

⑥ trap　当某些事件发生时，SNMP Agent 向 NMS 主动发出的消息。

执行前 4 种操作时设备使用 UDP 协议采用 161 端口发送报文，执行 Trap 操作时设备使用 UDP 协议采用 162 端口发送报文。由于收发采用了不同的端口号，所以一台设备可以同时作为 Agent 和 NMS。

■ SNMP 代理的功能

SNMP 代理用 get 报文来检测被管理对象的状况，用 set 报文来改变各被管对象的状况。也就是说，SNMP 代理以下述两种方式回应 NMS 的请求：

① Get 一个 MIB 变量——SNMP 代理回应来自 NMS 的请求时开始启用该功能。Agent 从请求的 MIB 变量中获取数值，并将其反馈给 NMS。

② Set 一个 MIB 变量——SNMP 代理回应来自 NMS 的消息时开始启用该功能。Agent 将 MIB 变量值修改为 NMS 的请求值。

SNMP 代理也主动发送陷阱消息，以通知 NMS 在 Agent 上已经发生了重要事件。

■ SNMP 字符串

SNMP 字符串像嵌入的密码一样，用于认证对 MIB 对象和特性的访问。NMS 若欲访问交换机，其字符串必须与交换机上定义的三个字符串中的至少一个完全相同。

字符串可有下列属性之一：

① Read-only（RO）——赋予认证管理工作站读取访问 MIB 所有对象（团体字符串除外）的权利，但是，不允许写访问。

② Read-wirte（RW）——赋予认证管理工作站读取和写入访问 MIB 所有对象的权利，但是，不允许访问团体字符串。

③ Read-wirte-all——赋予认证管理工作站读取和写入访问 MIB 所有对象的权利，包括团体字符串。

■ SNMP 的技术特点

SNMP 具有以下技术优点：

① 基于 TCP/IP 互联网的标准协议，传输层协议一般采用 UDP。

② 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。

③ 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务与被管设备的物理特性和实际网络类型相对独立，从而实现对不同厂商设备的管理。

④ 简单的请求—应答方式和主动通告方式相结合，并有超时和重传机制。

⑤ 报文种类少，报文格式简单，方便解析，易于实现。

⑥ SNMPv3 版本提供了认证和加密安全机制，以及基于用户和视图的访问控制功能，增强了安全性。

2. SNMP 默认配置

表 7-3 显示了 SNMP 的默认配置。

表 7-3　SNMP 默认配置

特　　性	默认设置
SNMP 代理	启用
SNMP 陷阱接收	未配置
SNMP 陷阱	未启用，TCP 连接（tty）陷阱除外
SNMP 版本	如果没有 version 关键字出现，默认是版本 1
SNMPv3 认证	如果没有输入关键字，默认是 noauth（noAuthNoPriv）安全级别
SNMP 通知类型	如果没有指定类型，所有通知都将被发送

3. SNMP 配置策略

配置 SNMP 时，应当遵循以下策略：

- 一个 SNMP 组是映射 SNMP 用户至 SNMP 视图的一张表。SNMP 用户是 SNMP 组的成员。SNMP 主机是 SNMP 陷阱操作的接受者。SNMP Engine ID 是本地或远程 SNMP 引擎的名称。在配置 SNMP 时，应当遵循以下策略。
- 在配置 SNMP 组时，不要指定通知视图。Snmp-server host 全局配置命令将自动生成通知视图，并将其与用户一起添加至组。修改组通知视图将会对组内的所有用户都产生影响。
- 配置远程用户时，需要为远程设备的 SNMP 代理指定 IP 地址或端口号。
- 在为远程用户配置特别代理之前，需要使用带有 remote 选项的 snmp-server engineID 全局配置命令配置 SNMP 引擎 ID。远程代理的 SNMP 引擎 ID 和用户密码被用于安全认证。如果没有预先配置远程引擎 ID，配置命令将会失败。
- 当配置 SNMP 通知时，需要为 SNMP 数据库中的远程代理配置 SNMP 引擎 ID，以发送代理请求或通知。
- 如果本地用户没有关联至远程主机，交换机将不发送认证级别的 auth (authNoPriv)和 priv (authPriv)通知。
- 修改 SNMP 引擎 ID 值会产生重要影响。用户密码（在命令行输入）将转换为基于密码和本地引擎 ID 的 MD5 或 SHA 安全摘要，原命令行密码被删除。引擎 ID 数值被修改时，SNMPv3 用户的安全摘要将会无效，需要使用 snmp-server user *nsername* 全局配置命令重新配置 SNMP 用户。同样，团体字符串也需要重要配置。

4. 禁用 SNMP 代理

在全局配置模式下，使用 no snmp-server 命令，即可禁用 SNMP 代理。

7.3.3 配置 RMON

RMON（Remote Monitor）远程监控是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据，为网络管理员选择符合指定网络需求的控制台和网络监控探测器提供了更多的自由。

1. RMON 默认配置

交换机 RMON 支持 SNMP 的 1、2、3、9 组内容。

- 统计组。统计组（statistics）是 RMON 中的第 1 组，统计组统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控和统计。
- 历史组。历史组（history）是 RMON 中的第 2 组，历史组定期地收集统计网络值的记录并为日后的处理把统计存储起来。它包含两个小组。其中，HistoryControl 组用来设置采样间隔时间等控制信息；EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率，以及碰撞次数等其他统计信息的历史数据。
- 警报组。警报组（alarm）是 RMON 中的第 3 组，以指定的时间间隔监控一个特定的 MIB（Management Information Base）对象，当这个 MIB 对象的值超过一个设定的上限值或低于一个设定的下限值时，会触发一个警报。警报被当作事件来处理，处理事件的方式可以是记录日志或发送 SNMP Trap（陷阱）的方式。
- 事件组。事件组（event）是 RMON 中的第 9 组，决定当由于警报而产生事件时，处理行为产生一个日志记录表项或者一个 SNMP Trap。

RMON 在默认情况下是禁用的，警告和过滤都没有被配置。在交换机上只有 RMON1 被支持。

2. 配置 RMON 警报和事件

可以使用 CLI 或 SNMP 网络管理工作站配置交换机 RMON。建议使用 NMS（网络管理工作站）上的一般的 RMON 管理工具来实现 RMON 的管理，以便充分利用 RMON 的网络管理功能。当然，也必须在交换机上配置 SNMP 以访问 RMON MIB 对象。

在特权 Exec 模式下开始，启用 RMON 警告和过滤。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 设置针对一个 MIB 对象的报警功能。number 用于指定这个 alarm 表项的索引，取值范围是 1～65535。Variable 表示要监控的 MIB 的变量标识符，该变量必须是整型类数据类型。interval 用于指定采样的时间间隔，单位为秒，取值范围为 1～2147483647s。关键字 delta 表示取样的值，指 MIB 变量在两次取样间值的变化；关键字 absolute 表示直接使用 MIB 变量的值作为取样值。Value 用于指定警报触发的条件，即当 MIB 变量的值变化成大于关键字 rising-threshold 后面指定的 value 值（从小于这个值变成大于这个值），或者变成小于关键字 falling-threshold 后面指定的 value 值时即触发警报。Value 后所跟的值取值范围是-2 147 483 648～2 147 483 647。event-number（可选）表示报警引发的事件产生时，指定事件组产生事件表项的索引，若不指定则不会产生相应的事件。这个值的取值范围为 1～65 535。string（可选）用于标识这个报警表项的拥有者。

```
Switch（config） # rmon alarm number variable interval {absolute | delta}
rising-threshold value [event-number] falling-threshold value [event-number]
[owner string]
```

③ 当警报产生时，增加相应的事件表项并做相应的处理。number 表示事件表项的索引，

和上面设置的 event-number 对应。一个警报产生时，若警报指定的 event-number 对应的事件表项（number 等于 event-number）不存在，则不会产生对应的事件。该值的取值范围为 1～65 535。Log（可选）输入这个关键值，则警报产生时，会将这个事件记录到日志中。trap（可选）输入这个关键值，则警报产生时，会产生一个 SNAP Trap。community（可选）发送 Trap 时使用的认证名。description string（可选）对这个事件的描述。owner string（可选）标志这个事件的拥有者。

```
Switch (config) # rmon event number [description string] [log] [owner string]
[trap community]
```

④ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑤ 校验配置。

```
Switch # show running-config
```

⑥ 保存配置。

```
Switch # copy running-config startup-config
```

禁用警告，使用“**no rmon alarm** *number*”全局配置命令，不能立即禁用所有已配置的警告。禁用事件，使用“**no rmon even**t *number*”全局配置命令。

3. 创建历史表组项

必须首先配置 RMON 警告和事件来显示收集的信息。

在特权 Exec 模式下开始，下面的步骤是在接口上创建历史表组项。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 指定要收集历史表的接口，并进入接口配置模式。

```
Switch (config) # interface interface-id
```

③ 创建历史表组项。Index 用于指定这个历史记录配置表项的索引，值的范围是 1～65 535。owner ownername（可选）标志这个表项的拥有者。buckets 表示每次采样的数据将被保存下来，bucket-number 的值指定了保存每次采样数据的历史记录的最大表项个数。如果历史记录已满，则新的采样数据将覆盖最老的一次采样数据记录。取值范围是 1～65 535，默认值为 10。interval 指定采样的时间间隔，单位为秒，范围为 1～3 600 s，缺省为 1 800 s。

```
Switch (config-if) # rmon collection history index [buckets bucket-number]
[interval seconds] [owner ownername]
```

④ 返回特权 Exec 模式。

```
Switch (config-if) # end
```

⑤ 校验配置。

```
Switch # show running-config
```

⑥ 显示交换机历史中表的内容。

```
Switch (config) # show rmon history
```

⑦ 保存配置。

```
Switch # copy running-config startup-config
```

禁用历史收集，使用“**no rmon collection history** *index*”接口配置命令。

4. 创建 RMON 统计组表项

可以针对物理端口设置统计表项。当设置了一个端口的统计表项后，交换机将从这时开始各种数据的统计。

在特权 Exec 模式下，可以通过以下步骤来创建一个 RMON 统计组表项。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 指定创建统计组表项的接口，并进入接口配置模式。

```
Switch (config) # interface interface-id
```

③ 创建RMON统计组表项。index指定这个统计表项的索引，值的范围是1～65 535。owner ownername（可选）标志这个表项的拥有者。

```
Switch (config-if) # rmon collection stats index [owner ownername]
```

④ 返回特权 Exec 模式。

```
Switch (config-if) # end
```

⑤ 校验配置。

```
Switch # show running-config
```

⑥ 显示交换机统计表的收集量。

```
Switch # show rmon statistics
```

⑦ 保存配置。

```
Switch # copy running-config startup-config
```

禁用以太网组统计量的收集，使用“**no rmon collection stats** *index*”接口配置命令。

5. 显示 RMON 的状态

使用下述命令，可以显示 RMON 的状态。

显示全部的 RMON 统计：

```
show rmon
```

显示 RMON 警告表：

```
show rmon alarms
```

显示 RMON 事件表：

```
show rmon events
```

显示 RMON 历史表：

```
show rmon history
```

显示 RMON 统计表：

```
show rmon statistics
```

7.3.4 配置 SPAN 和 RSPAN

使用 SPAN（Switched Port Analyzer）或者 RSPAN（Remote SPAN）可以有效地分析通过端口或 VLAN 的网络流量。借助 SPAN 或 RSPAN，可以将一个交换机的端口映像至另一个交换机端口，即发送流量的备份到该交换机或者其他交换机的另一个端口，这样只需将分析或侦听设备连接至监控端口，即可实现对被监听端口的分析和侦听。由于 SPAN 采用复制（或镜像）源端口或源 VLAN 上的接收或发送（或两者都有的）流量到目的端口，因此 SPAN 不影响源端口或 VLAN 的网络交换。事实上，除了 SPAN 或 RSPAN 会话所需的流量之外，目的端口不会接收或转发流量。

1. SPAN 和 RSPAN 简介

对单个或多个交换机端口进行监控和故障查寻，不需要中断现有业务流量，有助于故障隔离。交换式端口分析器（SPAN）分析经过某个本地端口或 VLAN 的流量信息。然后，SPAN 发送一份流量的副本给连接安全设备的交换机端口。

> **注意** 一旦启用了 SPAN、VSPAN 或 RSPAN，目标端口的 STP 就被禁止，可能会造成环路。另外，配置 RSPAN 之前要先定义一个 RSPAN 专用的 VLAN。如果在 VTP 服务器上配置了 RSPAN VLAN，那么 VTP 服务器自动将正确的信息传播给其他中间交换机。否则，要确保每台中间交换机都配置有 RSPAN VLAN。

■ **SPAN 术语**

- 入口业务：进入交换机的业务。
- 出口业务：离开交换机的业务。
- 源（SPAN）端口：用 SPAN 功能受监控的端口。
- 目的地（SPAN）端口：监控源端口的端口，通常连有一个网络分析器。
- 监控端口：监控端口也是目的地 SPAN 端口。
- 管理源：已配置受监控的源端口或者 VLAN 的列表。
- 操作源：受到有效监控的端口列表。这可能与管理源有所不同。例如，在关闭模式下的端口可能在管理源中出现，但它不受有效监控。

■ **SPAN 模式**

SPAN 拥有以下 3 种模式。

- 本地 SPAN：也称 PSPAN，指基于端口的 SPAN。源端口和目的端口都处于同一交换机（如图 7-23 所示），并且源端口可以是一个或多个交换机端口。

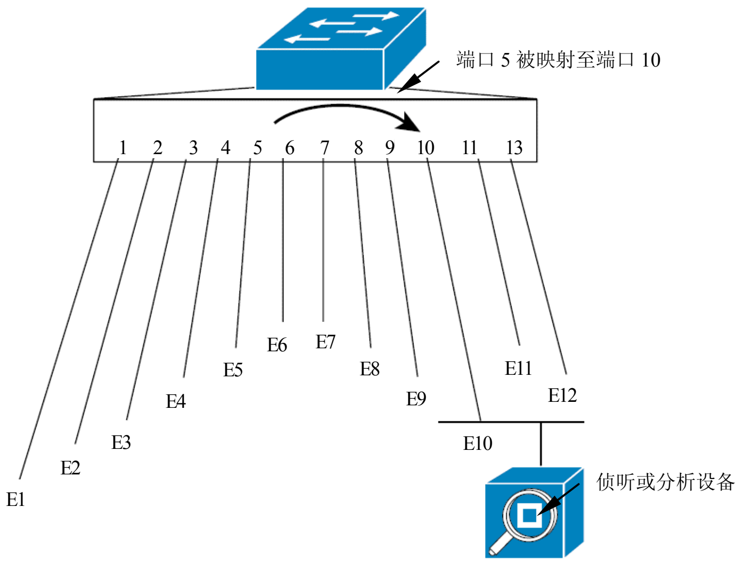


图 7-23　SPAN 示意图

- 远程 SPAN 或者 RSPAN：目的端口的源端口没有位于同一交换机上（如图 7-24 所示）。这是一项高级功能，要求有专门的 VLAN 来传送该业务，并由交换机之间的 SPAN 进行监控，因此，要求中间交换机必须支持 RSPAN VLAN 技术。由此可见，并非所有交换机均支持 RSPAN。所以应检查各自的版本说明或者配置指南，核实要进行配置的交换机是否可以使用该功能。

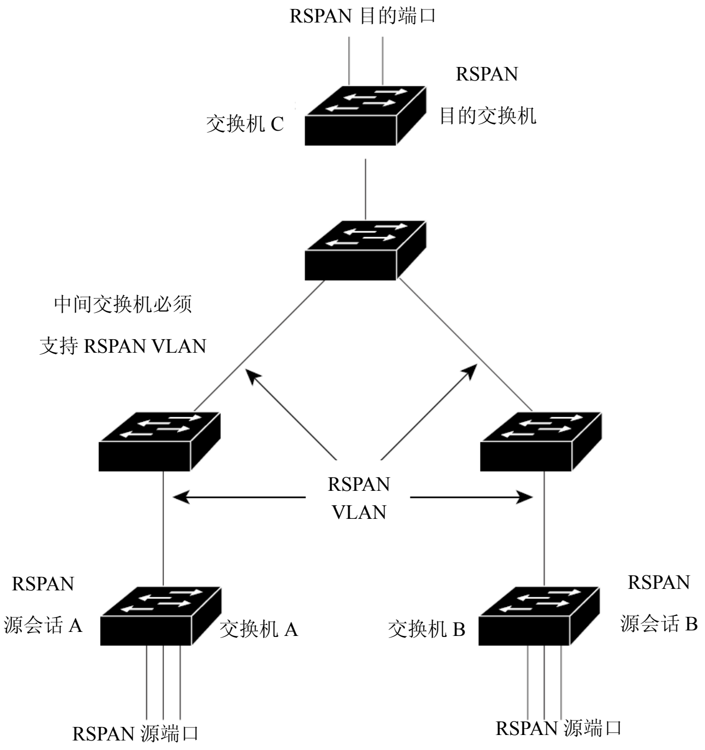


图 7-24　RSPAN 示意图

- VSPAN：指基于 VLAN 的 SPAN。SPAN 的一种变体，源端口不是物理端口，而是 VLAN。在给定的交换机中，用户可以使用单个命令来选择对属于专门 VLAN 的所有端口进行监控。

2. SPAN 和 RSPAN 默认配置

表 7-4 显示了 SPAN 和 RSPAN 的默认配置。

表 7-4 SPAN 和 RSPAN 默认配置

特　性	默认设置
SPAN 状态（SPAN 和 RSPAN）	禁用
源端口流量监控	接收并发送
封装类型（目的端口）	本地形式（不带标记的数据包）
转发（目的端口）	禁用
VLAN 过滤	在作为源端口的中继接口上，允许所有的 VLAN
RSPAN VLAN	都被检测

3. SPAN 会话中的流量监视限制

- 源既可以是端口也可以是 VLAN，但不能将源端口和源 VLAN 混合放入一会话中。也就是说，VLAN 或端口应当分别位于不同的会话。同一会话中，要么是 VLAN，要么是端口，而不能既有端口又有 VLAN。
- 可以配置在每个交换机堆栈上的两个源会话（本地 SPAN 和 RSPAN 源会话）。在同一台交换机上，可以同时运行一个本地 SPAN 和一个 RSPAN。源和 RSPAN 目的会话的总数不能超过 66 个。
- 在一个 SPAN 会话中，可以有多个目的端口，但最多不能超过 64 个目的端口。
- 借助分开或重叠配置的 SPAN 源端口和 VLAN，可以配置两个分开的 SPAN 或 RSPAN 源会话。
- SPAN 会话不会干涉交换机的正常工作。但是，源端口与目的端口的速率应当尽量匹配，甚至目的端口的速率应当高于源端口。如果使用 100 Mbps 端口监视 1000 Mbps 端口，那么将导致端口宕掉或者丢失数据。
- 当 RSPAN 被启用时，一个被监视的包将发送两次，一次作为正常传输，一次作为监视包。因此，当监视大量的端口或 VLAN 时，将会大幅增加网络流量。
- 可以将禁用的端口配置为源或目的端口，但 SPAN 不会自动开始，直至目的端口和至少一个源端口或源 VLAN 被启用。
- 不能在一个会话中同时存在 SPAN 和 RSPAN。RSPAN 源会话不能有本地目的端口，RSPAN 目的会话也不能有一个本地源端口。在同一交换机上，一个 RSPAN 目的会话和一个 RSPAN 源会话用于同一 RSPAN VLAN 时，将不能运行。
- 交换端口和路由端口都能够被配置为 SPAN 源端口和目的端口。

4. 配置本地 SPAN

当监视源端口和目的端口都在同一台交换机上时，应当配置本地 SPAN。

■ **配置 SPAN 的配置策略**

当配置 SPAN 时遵循下面的策略。

- 对于源端口而言，既可以是一个端口或 VLAN，也可以是几个端口或 VLAN。但是在一个会话中，不能既有 VLAN 又有端口。
- 目的端口不能成为一个源端口，一个源端口也不能成为目的端口。
- 不能在同一个目的端口上有两个 SPAN 会话。
- 当配置一个交换机端口作为一个 SPAN 目的端口时，该交换机端口便不再是一个常规的交换机端口。只有监控的通信可以抵达 SPAN 目的端口。
- 将 10 Gbps 以太网模块端口配置为 SPAN 或 RSPAN 目的端口时，其连接速率可能会降低。
- 键入 SPAN 配置命令不能移除以前配置的 SPAN 参数。必须键入“**no monitor session** {*session_numbe*r | **all** | **local** | **remote**}”全局配置命令，才能删除已配置的 SPAN 参数。
- 对本地 SPAN 而言，如果“**encapsulation replicate**”关键字被指定，向外发送的数据包通过 SPAN 目的端口时，将携带初始封装报头——未标记的 ISL 或 IEEE802.1q。如果该关键字没有被指定，数据包就会以本地模式发送。对于 RSPAN 目的端口，向外发送的数据是没有被标记的。
- 可以限制 SPAN 通信到指定的 VLAN，使用“**filter vlan**”关键字。如果一个汇聚端口被监控，只有具有关键字的在指定的 VLAN 上的通信才可以被监控。默认情况下，所有在中继端口上的 VLAN 都被监控。

■ **创建本地 SPAN 会话**

创建一个 SPAN 会话，并且指定源端口或 VLAN，以及目的端口。下述操作从特权 Exec 模式下开始。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 在对话中移除所有存在的 SPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local |remote}
```

③ 指定 SPAN 会话和源端口（被监视端口）。*session_number* 可取值范围为 1～66，*interface-id* 端口号的有效取值范围为 1～48。*vlan-id* 可取值范围为 1～4094。Both 表示同时监视进/出双向流量，Rx 表示仅监控入口流量；Tx 表示仅监控出口流量。

```
Switch (config) # monitor session session_number source {interface interface-id |vlan vlan-id} [, |-] [both |rx |tx]
```

④ 指定 SPAN 会话和目的端口（监视端口）。

```
Switch (config) # monitor session session_number destination {interface interface-id [,|-] [encapsulation replicate]}
```

⑤ 返回特权 Exec 模式。

```
Switch (config-if) # end
```

⑥ 校验配置。

```
Switch # show monitor [session session_number]
```

```
Switch # show running-config
```

⑦ 保存当前配置。

```
Switch # copy running-config startup-config
```

要删除一个 SPAN 会话，使用“**no monitor session** *session_number*”全局配置指令。移除来自一个 SPAN 会话的源或者目的端口或者 VLAN，使用“**no monitor session** *session_number* **source** {**interface** *interface-id* |**vlan** *vlan-id*}”全局配置命令，或者“**no monitor session** *session_number* **destination interface** *interface-id*”全局配置指令。对于目的接口封装选项和没有形式的命令都被忽略。

■ **创建本地 SPAN 会话并配置流量**

在特权 Exec 模式下开始，创建一个 SPAN 会话，指定源端口或目的端口，并且在目的端口为一个网络安全设备启用流量控制。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 为会话移除所有已存在的 SPAN 配置。

```
Switch (config) # no monitor session {session_number |all | local | remote}
```

③ 指定 SPAN 会话和源端口（被监视端口）。

```
Switch (config) # monitor session session_number source {interface interface-id
| vlan vlan-id} [,|-] [both | rx |tx]
```

④ 指定 SPAN 会话、目的端口、封装包和 VLAN 封装。

```
Switch (config) # monitor session session_number destination {interface
interface-id [,| -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl
|untagged vlan vlan-id |vlan vlan-id}]}
```

⑤ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑥ 校验配置。

```
Switch # show monitor [session session_number]
Switch # show running-config
```

⑦ 保存配置。

```
Switch # copy running-config startup-config
```

要删除一个 SPAN 会话，使用“**no monitor session** *session_number*”全局配置指令。要移除一个源或者目的端口或者来自 SPAN 会话的 VLAN，使用“**no monitor session** *session_number* **source** {**interface** *interface-id* |**vlan** *vlan-id* }”全局配置指令，或者“**no monitor session** *session_number* **destination interface** *interface-id* ”全局配置指令。对于目的接口，封装选项和没有形式的命令都被忽略。

■ **指定过滤 VLAN**

在特权 Exec 模式下，限制到指定 VLAN 的 SPAN 源流量。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 为会话移除已存在的所有的 SPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local | remote}
```

③ 指定源端口的特性和 SPAN 会话。

```
Switch (config) # monitor session session_number source interface interface-id
```

④ 限制到指定 VLAN 的 SPAN 源流量。

```
Switch (config) # monitor session session_number filter vlan vlan-id [,|-]
```

⑤ 指定 SPAN 会话和目的端口（监视端口）。

```
Switch (config) # monitor session session_number destination {interface interface-id [,|-] [encapsulation replicate]}
```

⑥ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑦ 校验配置。

```
Switch # show monitor [session session_number]
Switch # show running-config
```

⑧ 保存配置。

```
Switch (config) # copy running-config startup-config
```

检测中继端口上的 VLAN，使用“**no monitor session** *session_number* **filter**”全局配置命令。

5. 配置 RSPAN

■ **RSPAN 的配置策略**

下面是配置 RSPAN 的配置策略。

- 由于 RSPAN 必须借助 RSPAN VLAN 才能实现，因此应该在网络中为 RSPAN VLAN 预留少量 VLAN，并且不要将端口指定至这些 VLAN。
- 可以将一个输出 ACL 应用到 SRPAN 通信，从而选择性地过滤或监控指定的数据包。在 RSPAN 源交换机上的 RSPAN VLAN 中应用这些 ACL。
- 对 RSPAN 配置而言，源端口和目的端口可以跨越网络中的多个交换机。
- RSPAN 不支持 BPDU 包监控或其他二层交换机协议。
- RSPAN VLAN 只能在中继端口而不是访问端口配置。避免 RSPAN VLAN 中不必要的通信，确保所有涉及到的交换机都能支持 VLAN 远程 SPAN 功能。
- RSPAN VLAN 上的所有访问端口（包括语音 VLAN 端口）都被设置为非活动状态。
- 当源中继端口有激活的 RSPAN VLAN 时，RSPAN VLAN 被包含作为源的基于端口的 RSPAN 会话中。RSPAN VLAN 也可以成为在 SPAN 会话中的源。

- 所有交换机中同一 RSPAN VLAN 应用于一个 RSPAN 会话，就可以将 VLAN 配置为 RSPAN VLAN：。所有参与的交换机都支持 RSPAN。
- 配置 RSPAN 源或目的会话之前，先配置一个 RSPAN VLAN。
- 如果启用 VTP 和 VTP 修剪，SRPAN 通信就会在汇聚端口被剪除。

■ 配置一个 VLAN 作为 RSPAN VLAN

在配置 RSPAN 之前，应当先创建一个新的 VLAN 作为 RSPAN VLAN，并且必须在所有参与到 RSPAN 的交换机上创建 RSPAN VLAN。如果 RSPAN VLAN-ID 在正常范围内（低于 1005）并且 VTP（VLAN Trunk Protocol，VLAN 中继协议）在网络中是启用状态，就可以在一个交换机上创建 RSPAN VLAN，这样在 VTP 域中，就可以创建多个 RSPAN VLAN 到其他交换机。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 键入一个 VLAN 号创建一个 VLAN，或者键入一个已存在的 VLAN 号，并且进入 VLAN 配置模式。

```
Switch (config) # vlan vlan-id
```

③ 配置 VLAN 作为 RSPAN VLAN。

```
Switch (config) # remote-span
```

④ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑤ 保存配置。

```
Switch# copy running-config startup-config
```

从一个 VLAN 中移除 RSPAN 特性，并且将其转为标准 VLAN，使用“**no remote-span**”VLAN 配置指令。

■ 创建 RSPAN 源会话

借助以下操作，可以创建一个 RSPAN 源会话。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为会话移除所有存在的 RSPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local | remote}
```

③ 指定 RSPAN 会话和源端口（被监视端口）。

```
Switch (config) # monitor session session_number source {interface interface-id
| vlan vlan-id} [,|-] [both |rx |tx]
```

④ 指定 RSPAN 会话和目的 RSPAN VLAN。

```
Switch (config) # monitor session session_number destination remote vlan vlan-id
```

⑤ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑥ 校验配置。

```
Switch # show monitor [session session_number]
Switch # show running-config
```

⑦ 保存配置。

```
Switch # copy running-config startup-config
```

删除一个 SPAN 会话，使用“**no monitor session** *session_number*”全局配置命令。移除一个源端口或者来自 SPAN 会话的 VLAN，使用“**no monitor session** *session_number* **source {interface** *interface-id* **|vlan** *vlan-id***}**”全局配置命令。从会话中移除 RSPAN VLAN，使用“**no monitor session** *session_number* **destination remote vlan** *vlan-id*”。

删除一个 SPAN 会话，使用“**no monitor session** *session_number*”全局配置指令。移除一个源端口或者来自 SPAN 会话的 VLAN，使用“**no monitor session** *session_number* **source {interface** *interface-id* **|vlan** *vlan-id***}**”全局配置指令。要从一个会话移除 RSPAN VLAN，使用“**no monitor session** *session_number* **destination remote vlan** *vlan-id*”。

■ **创建 RSPAN 目的会话**

在其他交换机或交换机堆栈上配置 RSPAN 目的会话，也就是说，不能在源对话交换机或交换机堆栈上配置目的会话。在特权 Exec 模式下开始，执行下述操作可以在交换机上定义 RSPAN VLAN，创建一个 RSPAN 目的会话并指定源 RSPAN VLAN 和目的端口。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 键入在源交换机上创建的 RSPAN VLAN 的 VLAN 号，并且进入 VLAN 配置模式。

```
Switch (config) # vlan vlan-id
```

③ 定义 VLAN 作为 RSPAN VLAN。

```
Switch (config) # remote-span
```

④ 返回全局配置模式。

```
Switch (config-if) # exit
```

⑤ 为会话移除所有存在的 RSPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local| remote}
```

⑥ 指定 RSPAN 会话和源 RSPAN VLAN。

```
Switch (config) # monitor session session_number destination interface
interface-id
```

⑦ 指定 RSPAN 会话和目的接口。

```
Switch (config) # monitor session session_number destination interface
interace-id
```

⑧ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑨ 校验配置。

```
Switch # show monitor [session session_number]
Switch # show running-config
```

⑩ 保存配置。

```
Switch # copy running-config startup-config
```

要删除会话，使用“**no monitor session** *session_number*”全局配置命令。移除来自 SPAN 会话的目的端口，使用“**no monitor session** *session_number* **destination interface** *interface-id*”全局配置指令。移除来自会话的 RSPAN VLAN，使用“**no monitor session** *session_number* **source remote vlan** *vlan-id*”。

■ **创建 RSPAN 目的会话并配置流量**

在特权 Exec 模式下开始，创建一个 RSPAN 目的会话，指定源 RSPAN VLAN 和目的端口，并且在目的端口上为一个网络安全设备启用流量控制。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 为会话移除所有存在的 SPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local |remote}
```

③ 指定 RSPAN 会话和源 RSPAN VLAN。

```
Switch (config) # monitor session session_number source remote vlan vlan-id
```

④ 指定 SPAN 会话，目的端口，封装包和 VLAN 封装。

```
Switch (config) # monitor session session_number destination {interface interface-id [,|-] [ingress {dot1q vlan vlan-id |isl |untagged vlan vlan-id |vlan vlan-id}]}
```

⑤ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑥ 校验配置。

```
Switch # show monitor [session session_number]
```

⑦ 保存配置。

```
Switch # copy running-config startup-config
```

删除一个 RSPAN 会话，使用“**no monitor session** *session_number*”全局配置命令。移除一个来自 RSPAN 会话的目的端口，使用“no monitor session *session_number* **destination interface** *interface-id*”全局配置命令。

■ **指定过滤 VLANs**

在特权 Exec 模式下开始，配置 RSPAN 源会话来限制 RSPAN 到指定 VLANs 的源流量。

① 进入全局配置模式。

```
Switch # configure terminal
```

② 为会话移除所有存在的 SPAN 配置。

```
Switch (config) # no monitor session {session_number |all |local | remote}
```

③ 指定源端口执行 SPAN 会话。

```
Switch (config) # monitor session session_number source interface interface-id
```

④ 限制 SPAN 源到指定 VLANs 的流量。

```
Switch (config) # monitor session session_number filter vlan vlan-id [,|-]
```

⑤ 指定 RSPAN 会话和目的远程 VLAN（RSPAN VLAN）。

```
Switch (config) # monitor session session_number destination remote vlan vlan-id
```

⑥ 返回特权 Exec 模式。

```
Switch (config) # end
```

⑦ 校验配置。

```
Switch # show monitor [session session_number]
Switch # show running-config
```

⑧ 保存配置。

```
Switch (config) # copy running-config startup-config
```

检测所有在中继端口上的 VLAN，使用“**no monitor session** *session_number* **filter vlan**”全局配置命令。

6. 显示 SPAN 和 RSPAN 状态

显示当前 SPAN 或者 RSPAN 的配置，使用“**show monitor**”用户 Exec 指令。也可以使用“**show running-config**”特权 Exec 指令显示已配置的 SPAN 或者 RSPAN 会话。

第 8 章　路 由 协 议

路由协议是路由器软件中的重要组成部分。路由器为互连的网络之间选择最佳的通信路径都是通过这些路由协议来完成的。路由协议的作用还在于建立以及维护路由表。路由表用于为每个 IP 包选择输出端口或下一跳地址。

8.1　静态路由与默认路由

8.1.1　直连路由

直接连接到路由器接口的子网称为直连子网。路由器自动将其路由加入路由表，称为直连路由（Connected）。也就是说，当接口处于“up up”状态时，该接口所在的本地直连子网路由将被加入至路由表。图 8-1 所示为直连路由。

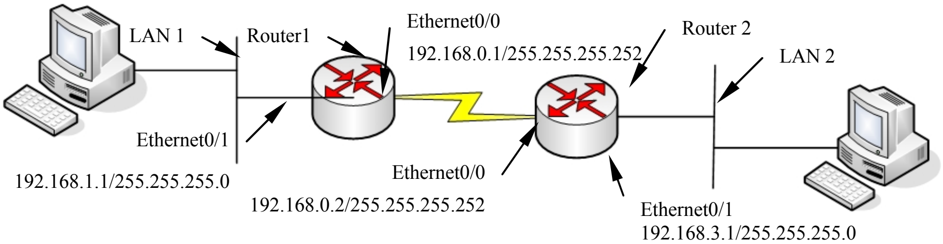


图 8-1　直连路由

图 8-2 所示为 Router1 的路由表。可见，其路由表中只包含 2 条连接至对端路由器和交换机的直连路由（C - connected）。

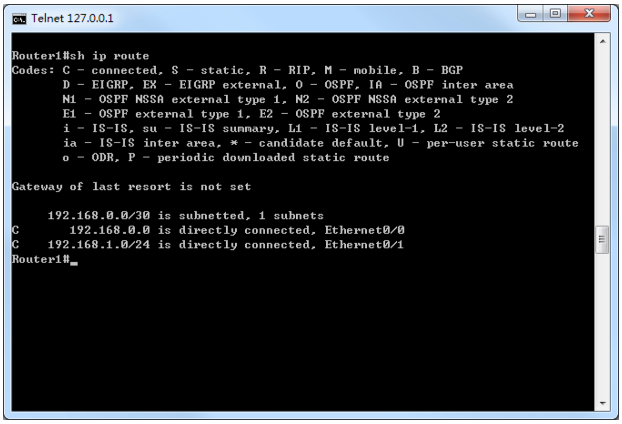


图 8-2　Router1 的路由表

路由器的路由表将列出路由器所有已知 IP 网络和子网，以及将数据包发往这些网络的出口，从而实现 IP 网络和子网间的路由。

8.1.2 静态路由

静态路由是在路由器中设置固定的路由表，即指定固定的传输路径，除非网络管理干预，否则将不会自动更改。所以当网络的拓扑结构或链路的状态发生变化时，需要手工修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。

静态路由是一种特殊的路由，它由管理员手工配置而成。通过静态路由的配置可建立一个互边的网络，但这种配置的问题在于：当一个网络故障发生后，静态路由不会自动发生改变，必须有管理员的介入。

在组网结构比较简单的网络中，只需配置静态路由就可以使路由器正常工作，仔细设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由还有如下的属性。

- 可达路由：正常的路由都属于这种情况，即 IP 报文按照目的地标识的路由被送往下一跳，这是静态路由的一般用法。
- 目的地不可达的路由：当到某一目的地的静态路由具有“丢弃”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且通知源主机目的地不可达。
- 目的地为“黑洞”的路由：当到某一目的地的静态路由具有“黑洞”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且不通知源主机。

其中，“丢弃”和“黑洞”属性一般用来控制本路由器可达目的地的范围，辅助网络故障的诊断。

通过配置静态路由，可以人为地指定对某一网络访问时所要经过的路径。在网络结构比较简单，并且到达某一网络只有唯一路径时，均采用静态路由。静态路由的效率最高，系统性能占用最少。对于企业网络而言，往往只有一条连接至 Internet 的链路，因此最适合使用静态路由。

例如，在如图 8-3 所示的网络中，如果用户访问该网络时必须经过路由器 A 和路由器 B，则管理员可以在路由器 A 中设置一条指向路由器 B 的静态路由信息。这样做的好处是可以减少路由器 A 和路由器 B 之间 WAN 链路上的数据传输量，因为网络在使用静态路由后，路由器 A 和路由器 B 之间没有必要进行路由信息的交换。

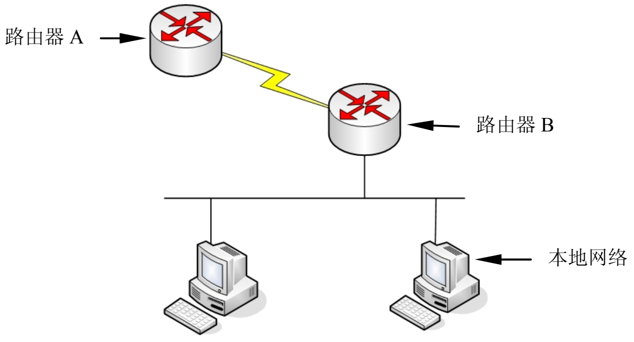


图 8-3　静态路由选择

以静态路由中的示例为例，若欲实现 LAN1 对 LAN2 的访问，则应当键入如下命令：

```
ip route 192.168.3.0 255.255.255.0 Ethernet0/0
```

即将对 LAN2 的访问全部路由至 Router1 的 Ethernet0/0 接口。添加静态路由（S - static）后，Router1 的路由表如图 8-4 所示。

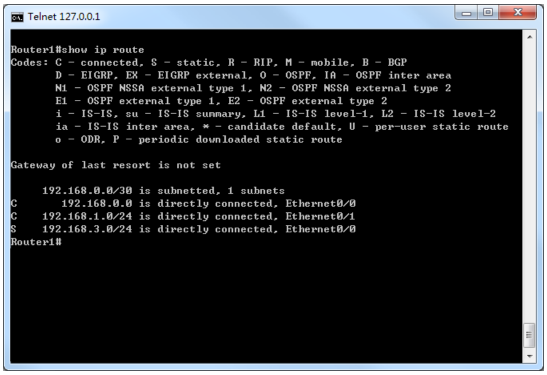


图 8-4　Router1 静态路由表

8.1.3 默认路由

默认路由是一种特殊的路由，可以通过静态路由配置，某些动态路由协议也可以生成默认路由，如 OSPF。

简单地说，默认路由就是在没有找到匹配的路由表入口项时才使用的路由。即只有当没有合适的路由时，默认路由才被使用。在路由表中，默认路由以到网络 0.0.0.0（掩码为 0.0.0.0）的路由形式出现。如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取默认路由。

既可以将默认路由设置为某个 IP 地址，也可以将其设置为某个接口。默认路由的命令格式为：

```
ip route 0.0.0.0 0.0.0.0 defautl_gate_ipaddress
ip route 0.0.0.0 0.0.0.0 defautl_gate_interface
```

如果没有默认路由且报文的目的地不在路由表中，那么该报文被丢弃的同时，将向源端返回一个 ICMP 报文报告该目的地址或网络不可达。

如图 8-5 所示为默认路由拓扑结构，若欲实现局域网络对所有未知网络的访问，就必须设置默认路由。

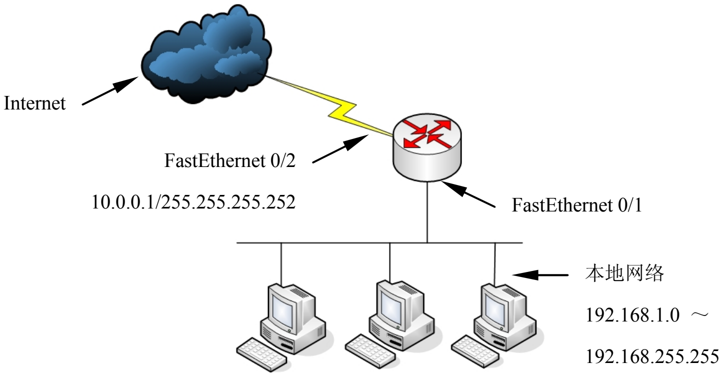


图 8-5　默认路由拓扑结构

默认路由的相应配置命令为：

```
ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

或者

```
ip route 0.0.0.0 0.0.0.0 fastethernet f0/2
```

8.2 动态路由协议

路由协议是用于路由器之间交换路由信息的协议。通过路由协议，路由器可以动态共享有关远程网络的信息。动态路由协议可以自动的发现远程网络，确定到达各个网络的最佳路径，然后将路径添加到路由表中。因此，借助动态路由协议，只要网络拓扑结构发生了变化，路由器就会相互交换路由信息，不仅能够自动获知新增加的网络，还可以在当前网络连接失败时找出备用路径。

8.2.1 RIP 路由协议

RIP（Routing Information Protocol，路由信息协议）作为一种较为简单的动态路由协议，在 AS（Autonomous System，自治系统）系统实际使用中有着广泛的应用。RIP 协议是一个应用于网关（路由器）和主机之间交换路由器信息的距离矢量协议，目前最新版本是 RIP v2。RIP 采用距离矢量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到了全网。

1. RIP 工作机制

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它使用 UDP 报文进行路由信息的交换。RIP 使用跳数（Hop Count）来衡量到达宿机的距离，称为路由权（Routing Metric）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定路由权取值为 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

RIP 每隔 30 s 发送一次路由刷新报文，如果在 180 s 内收不到从某一网络邻居发来的路由刷新报文，则将该网络邻居的所有路由标记为不可达。如果在 240 s 之内收不到从某一网上邻居发来的路由刷新报文，则将该网络邻居的路由从相应协议路由表中清除。

为提高性能，防止产生路由环，RIP 支持水平分割（Split Horizon）和毒性逆转（Poison Reverse）。RIP 还可引入其他路由协议所得到的路由。

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到网络所有可达信宿的路由项，这些路由项包含下列信息。

- 目的地址：指主机或网络的地址。
- 下一跳地址：指为到达目的地，本路由器要经过的下一个路由器地址。
- 接口：指转发报文的接口。
- metric 值：指本路由器到达目的地的开销，是一个 0～16 之间的整数。
- 定时器：从路由项最后一次被修改到现在所经过的时间，路由项每次被修改时，定时器重置为 0。
- 路由标记：区分路由为内部路由协议的路由还是外部路由协议的路由的标记。

2. RIP 的启动和运行

RIP 启动和运行的整个过程可描述如下。

- 某路由器刚启动 RIP 时，以广播或组播的形式向相邻路由器发送请求报文，相邻路由器的 RIP 收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文。
- 路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在一连串的触发修改广播后，各路由器都能得到并保持最新的路由信息。
- 同时，RIP 每隔 30 s 向相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。

3. RIPv1 和 RIPv2

RIP 有 RIPv1 和 RIPv2 两个版本，可以指定接口所处理的 RIP 报文版本。RIPv2 由 RIPv1 而来，属于 RIP 协议的补充协议，主要用于扩大装载的有用信息的数量，同时增加其安全性能。RIPv1 和 RIPv2 都是基于 UDP 的协议。在 RIPv2 下，每台主机或路由器通过路由选择进程发送和接受来自 UDP 端口 520 的数据包。

RIPv1 的报文传送方式为广播方式。RIPv2 有两种报文传送方式，即广播方式和组播方式，默认将采用组播方式发送报文，减少网络与系统资源消耗。RIPv2 中组播地址为 224.0.0.9。组播发送报文的好处是在同一网络中那些没有运行 RIP 的主机可以避免接收 RIP 的广播报文。另外，以组播方式发送报文还可以使运行 RIPv1 的主机避免错误地接收和处理 RIPv2 中带有子网掩码的路由。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。

RIPv1 是有类路由协议，RIPv2 是无类路由协议，即 RIPv2 的报文中含有掩码信息，支持 VLSM（可变长子网掩码）和 CIDR（Classless Inter-Domain Routing，无类域间路由）。

RIPv2 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

RIPv1 和 RIPv2 的区别如表 8-1 所示。

表 8-1　RIPv1 和 RIPv2 的区别

RIPv1	RIPv2
有类路由	无类路由
不支持 VLSM	支持 VLSM
广播更新（255.255.255.255）	组播更新（224.0.0.9）
自动汇总，不支持手动汇总	自动汇总，且可以手动关闭该特性。支持手动汇总
不支持验证	支持验证
产生 CIDR	不产生 CIDR

4. RIP 协议的特点

RIP 协议有以下特点：

- RIP 是自治系统内部使用的协议即内部网关协议（IGP，Interior Gateway Protocol），使用的是距离矢量算法。
- RIP 使用 UDP 的 520 端口进行 RIP 进程之间的通信。

- RIP 协议以跳数作为网络度量值。
- RIP 协议的网络直径不超过 15 跳，适合于中小型网络。16 跳时认为网络不可达。
- RIP 协议支持主机被动模式，即 RIP 协议允许主机只接收和更新路由信息而不发送信息。
- RIP 协议支持默认路由传播。

5. RIP 协议优缺点

RIP 协议的优点是简单、可靠，配置简单，非常适用于小规模网络。对于复杂环境及大型网络，一般不使用 RIP。

RIP 协议的缺点包括：

- 大量广播。RIP 向所有邻居每隔 30 s 广播一次完整的路由表，将占用宝贵的带宽资源，在较慢的广域网链路上问题尤为严重。
- 没有成本概念。RIP 没有网络延迟和链路成本的概念。当采用 RIP 时，路由/转发的决定只是基于跳数，这样很容易导致无法选择最佳路由。例如，一条链路拥有较高的带宽，但是跳数较多，从而不能被选择。
- 支持的网络规模有限。由于 RIP 最多只支持 16 个步跳，当超过该跳数时，网络将认为无法到达。因此，RIP 只能适用于规模较小的网络。
- 收敛性差，时间经常大于 5 分钟。

8.2.2 OSPF 路由协议

20 世纪 80 年代中期，RIP 已不能适应大规模异构网络的互连，OSPF（Open Shortest Path First，开放最短路径优先）路由协议随之产生。它是网间工程任务组织（IETF）的内部网关协议工作组为 IP 网络而开发的一种路由协议。

1. OSPF 路由协议简介

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。

开放最短路由优先协议 OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议。目前使用的是 OSPFv2（RFC2328），其特性如下。

- 适应范围。支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛。在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环。由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分。允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。

- 等值路由。支持到同一目的地址的多条等值路由。
- 路由分级。使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第 1 类外部路由、第 2 类外部路由。
- 支持验证。支持基于接口的报文验证以保证路由计算的安全性。
- 组播发送。支持组播地址。

2. OSPF 路由计算过程

每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统拓扑结构的链路状态数据库 LSDB（Link State Database）。每台路由器根据自己周围的网络拓扑结构生成链路状态广播 LSA（Link State Advertisement），通过相互之间发送协议报文将 LSA 发送给网络中其他路由器。这样每台路由器都收到了其他路由器的 LSA，所有的 LSA 放在一起便组成了链路状态数据库。

OSPF 路由协议利用链路状态算法建立和计算到每个目标网络的最短路径，该算法本身十分复杂，下面简单地、概括性地描述链路状态算法工作的总体过程。

- 初始化阶段，路由器将产生链路状态通告，该链路状态通告包含了该路由器全部链路状态。
- 所有路由器通过组播的方式交换链路状态信息，每台路由器接收到链路状态更新报文时，将复制一份到本地数据库，然后再传播给其他路由器。
- 当每台路由器都有一份完整的链路状态数据库时，路由器应用算法针对所有目标网络计算最短路径树，结果内容包括：目标网络、下一跳地址、花费，是 IP 路由表的关键部分。
- 如果没有链路花费、网络增删变化，OSPF 将会十分安静，如果网络发生了任何变化，OSPF 通过链路状态进行通告，但只通告变化的链路状态，变化涉及到的路由器将重新运行算法，生成新的最短路径树。

每台路由器都使用算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由，外部路由信息为叶子节点，外部路由可由广播它的路由器进行标记以记录关于自治系统的额外信息。显然，各个路由器各自得到的路由表是不同的。

此外，为使每台路由器能将本地状态信息（如可用接口信息、可达邻居信息等）广播到整个自治系统中，在路由器之间要建立多个邻接关系，这使得任何一台路由器的路由变化都会导致多次传递，既没有必要，也浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了“指定路由器”DR（Designated Router），所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。这样就减少了多址访问网络上各路由器之间邻接关系的数量。

3. OSPF 协议报文

OSPF 有 5 种报文类型。

- HELLO 报文（Hello Packet）。最常用的一种报文，周期性地发送给本路由器的邻居。内容包括一些定时器的数值、DR、BDR（Backup Designated Router），以及自己已知的邻居。
- DD 报文（Database Description Packet）。两台路由器进行数据库同步时，用 DD 报文来描述自己的 LSDB，内容包括 LSDB 中每一条 LSA 的摘要（摘要是指 LSA 的 HEAD，

通过该 HEAD 可以唯一标识一条 LSA）。这样做是为了减少路由器之间传递信息的量，因为 LSA 的 HEAD 只占一条 LSA 的整个数据量的一小部分，根据 HEAD，对端路由器就可以判断出是否已有这条 LSA。

- LSR 报文（Link State Request Packet）。两台路由器互相交换过 DD 报文之后，知道对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 的摘要。
- LSU 报文（Link State Update Packet）。用来向对端路由器发送所需要的 LSA，内容是多条 LSA（全部内容）的集合。
- LSAck 报文（Link State Acknowledgment Packet）。用来对接收到的 LSU 报文进行确认。内容是需要确认的 LSA 的 HEAD（一个报文可对多个 LSA 进行确认）。

4. OSPF 协议相关概念

路由器 ID 号

一台路由器如果要运行 OSPF 协议，必须存在 Router ID。如果没有配置 ID 号，系统会从当前接口的 IP 地址中自动选一个作为路由器的 ID 号。

DR 和 BDR

- 指定路由器 DR（Designated Router）。为使每台路由器能将本地状态信息广播到整个自治系统中，在路由器之间要建立多个邻居关系。但这使得任何一台路由器的路由变化都会导致多次传递，浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了 DR，所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。两台不是 DR 的路由器（称为 DR Other）之间将不再建立邻居关系，也不再交换任何路由信息。

> **提·示** 哪一台路由器会成为本网段内的 DR 并不是人为指定的，而是由本网段中所有的路由器共同选举出来的。

- 备份指定路由器 BDR（Backup Designated Router）。如果 DR 由于某种故障而失效，这时必须重新选举 DR，并与之同步。这需要较长的时间，在这段时间内，路由计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR 的概念。BDR 实际上是对 DR 的一个备份，在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR。

区域（Area）

一组运行 OSPF 路由协议的路由器，组成了 OSPF 路由域的自治域系统。一个自治域系统是指由一个组织机构控制管理的所有路由器，自治域系统内部只运行一种 IGP 路由协议，自治域系统之间通常采用 BGP 路由协议进行路由信息交换。不同的自治域系统可以选择相同的 IGP 路由协议，如果要连接到因特网，每个自治域系统都需要向相关组织申请自治域系统编号。

随着网络规模日益扩大，当一个巨型网络中的路由器都运行 OSPF 路由协议时，路由器数量的增多会导致 LSDB 非常庞大，占用大量的存储空间，并使得运行 SPF 算法的复杂度增加，

导致 CPU 负担很重。并且，网络规模增大之后，拓扑结构发生变化的概率也会增大，网络会经常处于“动荡”之中，造成网络中会有大量的 OSPF 协议报文在传递，降低了网络的带宽利用率。而且每一次变化都会导致网络中所有的路由器重新进行路由计算。

当 OSPF 路由域规模较大时，一般采用分层结构，即将 OSPF 路由域分割成几个区域（AREA），区域之间通过一个骨干区域互连，每个非骨干区域都需要直接与骨干区域连接。

在 OSPF 路由域中，根据路由器的部署位置划分，有 3 种路由器角色。一是区域内部路由器，该路由器的所有接口网络都属于一个区域。二是区域边界路由器，也称为 ABR（Area Border Routers），该路由器的接口网络至少属于两个区域，其中一个必须为骨干区域。三是自治域边界路由器，也称为 ASBR（Autonomous System Boundary Routers），是 OSPF 路由域与外部路由域进行路由交换的必经之路。

■ **骨干区域和虚连接**

- 骨干区域（Backbone Area）。OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域是与众不同的，它的区域号（Area ID）是 0，通常被称为骨干区域。
- 虚连接（Virtual link）。由于所有区域都必须与骨干区域在逻辑上保持连接，特别引入了虚连接的概念，使那些物理上分割的区域仍可保持逻辑上的连通性。

■ **路由聚合**

AS 被划分成不同的区域，每一个区域通过 OSPF 边界路由器（ABR）相连，区域间可以通过路由汇聚来减少路由信息，减小路由表的规模，提高路由器的运算速度。

ABR 在计算出一个区域的区域内路由之后，查询路由表，将其中每一条 OSPF 路由封装成一条 LSA 发送到区域之外。

5. OSPF 协议优缺点

与 RIP 协议不同，OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式。当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其他区路由器的正常工作，这也给网络的管理、维护带来了方便。

■ **OSPF 协议主要优点**

OSPF 协议的主要优点如下。

- 快速收敛。OSPF 是真正的 LOOP-FREE（无路由自环）路由协议。源自其算法本身——链路状态及最短路径树算法，OSPF 具有收敛速度快，能够在最短的时间内将路由变化传递到整个自治系统。
- 区域划分。提出区域（Area）划分的概念，将自治系统划分为不同区域后，通过区域之间的对路由信息的摘要，大大减少了需传递的路由信息数量，也使得路由信息不会随网络规模的扩大而急剧膨胀。
- 开销控制。将协议自身的开销控制到最小。

① 用于发现和维护邻居关系的是定期发送的不含路由信息的 HELLO 报文，且非常短小。包含路由信息的报文是触发更新的机制，而且只有在路由变化时才会发送。但为了增强协议的健壮性，每 1 800 s 全部重发一次。

② 在广播网络中，使用组播地址（而非广播）发送报文，减少对其他不运行 OSPF 的网络设备的干扰。

③ 在各类可以多址访问的网络中（广播型网络，非广播型多路访问），通过选举 DR（指定路由器），使同网段的路由器之间的路由交换（同步）次数由 O（N×N）次减少为 O（N）次。

④ 提出 STUB 区域的概念，使得 STUB 区域内不再传播引入的 ASE 路由。

⑤ 在 ABR（区域边界路由器）上支持路由聚合，进一步减少区域间的路由信息传递。

⑥ 在点到点接口类型中，通过配置按需播号属性(OSPF over On Demand Circuits)，使得 OSPF 不再定时发送 HELLO 报文及定期更新路由信息。只在网络拓扑真正变化时才发送更新信息。

- 路由可信。通过严格划分路由的级别（共分 4 极），提供更可信的路由选择。
- 安全性高。良好的安全性，OSPF 支持基于接口的明文及 MD5 验证。
- 适应性广。OSPF 适应各种规模的网络，最多可达数千台。

■ OSPF 协议主要缺点

OSPF 协议的主要缺点如下。

- 配置相对复杂。由于网络区域划分和网络属性的复杂性，需要网络分析员有较高的网络知识水平才能配置和管理 OSPF 网络。
- 路由负载均衡能力较弱。OSPF 虽然能根据接口的速率、连接可靠性等信息，自动生成接口路由优先级，但在通往同一目的的不同优先级路由中，OSPF 只选择优先级较高的转发，不同优先级的路由，不能实现负载分担。只有相同优先级的，才能达到负载均衡的目的，不像 EIGRP 那样可以根据优先级不同，自动匹配流量。

8.2.3 EIGRP 路由协议

IGRP（Interior Gateway Routing Protocol，内部网关路由选择协议）是 Cisco 特有的基于距离矢量的路由协议，虽然同样应用于规模较小的局域网络，但与 RIP 路由协议有所不同，IGRP 使用 IP 层的端口号 9 进行报文交换，而 RIP 则使用 520 端口进行报文交换。

1. IGRP 与 EIGRP 路由协议

IGRP 同样是一种动态距离向量路由协议，它由 Cisco 公司 20 世纪 80 年代中期设计推出，使用跳数来确定到达一个网络的最佳路径，使用延迟、带宽、可靠性和负载来确定最优路由。默认状态下，IGRP 每 90 s 发送一次路由更新广播，在 3 个更新周期（即 270 s）内，没有从路由中的第一个路由器接收到更新，则宣布路由器不可访问。在 7 个周期（即 630 s）后，Cisco IOS 软件会从路由表中清除该路由。

EIGRP 是结合了链路状态和距离矢量型路由选择协议的 Cisco 专用协议，采用弥散修正算法（DUAL）来实现快速收敛，可以不发送定期的路由更新信息以减少带宽的占用，支持 Appletalk、IP 等多种网络层协议。自从 EIGRP 路由协议诞生后，IGRP 路由协议便很少再被使用了。

2. EIGRP 路由协议优缺点

■ EIGRP 路由协议主要优点

EIGRP 路由协议的主要优点如下。

- 精确路由计算和多路由支持。EIGRP 协议继承了 IGRP 协议最大的优点——矢量路由权。EIGRP 协议在路由计算中要对网络带宽、网络时延、信道占用率、信道可信度等因素作全面的综合考虑，所以 EIGRP 的路由计算更为准确，更能反映网络的实际情况。同时 EIGRP 协议支持多路由，使路由器可以按照不同的路径进行负载分担。
- 较少带宽占用。使用 EIGRP 协议的对等路由器之间周期性地发送很小的 HELLO 报文，以此来保证从前发送报文的有效性。路由的发送使用增量发送方法，即每次只发送发生变化的路由。发送的路由更新报文采用可靠传输，如果没有收到确认信息则重新发送，直至确认。EIGRP 还可以对发送的 EIGRP 报文进行控制，以减少 EIGRP 报文对接口带宽的占用率，从而避免连续大量发送路由报文而影响正常数据业务的事情发生。
- 快速收敛。无环路和路由的收敛速度是路由计算的重要指标。EIGRP 协议由于使用了 DUAL 算法，使得 EIGRP 协议在路由计算中不可能有环路路由产生，同时路由计算的收敛时间也有很好的保证。因为 DUAL 算法使得 EIGRP 在路由计算时，只会对发生变化的路由进行重新计算；对一条路由，也只有此路由影响的路由器才会介入路由的重新计算。
- MD5 认证。为确保路由获得的正确性，运行 EIGRP 协议进程的路由器之间可以配置 MD5 认证，对不符合认证的报文丢弃不理，从而确保路由获得的安全。
- 路由聚合。EIGRP 协议可以通过配置，对所有的 EIGRP 路由进行任意掩码长度的路由聚合，从而减少路由信息传输，节省带宽。
- 实现负载分担。去往同一目的的路由表项，可根据接口的速率、连接质量、可靠性等属性，自动生成路由优先级，报文发送时可根据这些信息自动匹配接口的流量，达到几个接口负载分担的目的。
- 配置简单。使用 EIGRP 协议组建网络，路由器配置非常简单，它没有复杂的区域设置，也无需针对不同网络接口类型实施不同的配置方法。使用 EIGRP 协议只需使用 router eigrp 命令在路由器上启动 EIGRP 路由进程，然后再使用 network 命令使用网络范围内的接口即可。

■ **EIGRP 路由协议主要缺点**

EIGRP 路由协议的主要缺点如下。

- 没有区域概念。EIGRP 没有区域（AREA）的概念，而 OSPF 在大规模网络的情况下，可以通过划分区域来规划和限制网络规模。所以 EIGRP 适用于网络规模相对较小的网络，这也是矢量距离路由算法（RIP 协议就是使用这种算法）的局限所在。
- 定时发送 HELLO 报文。运行 EIGRP 的路由器之间必须通过定时发送 HELLO 报文来维持邻居关系，这种邻居关系即使在拨号网络上，也需要定时发送 HELLO 报文，这样在按需拨号的网络上，无法定位这是有用的业务报文还是 EIGRP 发送的定时探询报文，从而可能误触发按需拨号网络发起连接，尤其在备份网络上，引起不必要的麻烦。
- 基于分布式的 DUAL 算法。EIGRP 的无环路计算和收敛速度是基于分布式的 DUAL 算法的，这种算法实际上是将不确定的路由信息（active route）散播（向邻居发 query 报文），得到所有邻居的确认后（reply 报文）再收敛的过程，邻居在不确定该路由信息可靠性的情况下又会重复这种散播，因此某些情况下可能会出现该路由信息一直处

于 active 状态（这种路由被称为 stuck in active route）。并且，如果在 active route 的这次 DUAL 计算过程中，出现到该路由的后继（successor）的 metric 发生变化的情况，就会进入多重计算，这些都会影响 DUAL 算法的收敛速度。

- EIGRP 是私有协议。Cisco 公司是该协议的发明者和唯一具备该协议解释和修改权的厂商。如果要支持 EIGRP 协议需向 Cisco 公司购买相应版权，而且 Cisco 公司修改该协议没有义务通知任何其他厂家和使用该协议的用户。

3. 常用动态路由协议比较

RIP 协议是典型的距离向量路由协议，算法简单，适合于网络拓扑结构相对简单、数据链路故障率低的小型网络。不过，在路径多时收敛速度慢，占用带宽资源多，因此，RIP 协议已不能适应大规模异构网络的互连。OSPF 作为一种链路状态路由协议，虽然能够适应大规模的网络，收敛速度快，但太复杂，执行时会占用较多的路由器资源和网络带宽。EIGRP 结合了 RIP 和 OSPF 两种协议优点，把 RIP 等旧路由协议的简单性和可靠性与 OSPF 等新一代路由协议的优点组合起来，使得 EIGRP 很容易配置和使用。

三种动态路由的特性比较如表 8-2 所示。

表 8-2　RIP、EIGRP 和 OSPF 特性比较

特　　性	RIP	OSPF	EIGRP
算法	距离矢量	链路状态	高级距离矢量
度量值	步跳	链路开销	带宽、延迟的函数
开放或专用标准	开放	开放	专用
周期的发送更新	是	否	否
全部或部分路由更新	全部	部分	部分
广播或组播发送更新	广播	组播	组播
被认为无穷大的度量值	16	16 777 215(2^{24}-1)	4 294 967 295(2^{32}-1)
支持非等值负载均衡	否	否	是

8.2.4 IS-IS 路由协议

在 ISO 规范中，一个路由器就是一个 IS（Intermediate System，中间系统），提供 IS 和 IS（路由器和路由器）之间通信的协议就是路由协议，即 IS-IS 路由协议。IS-IS 是一种链路状态协议，使用最短路径优先（Shortest Path First，SPF）算法，与 OSPF 协议有很多相似之处。IS-IS 属于内部网关协议，用于自治系统内部。

1. IS-IS 路由协议相关概念

■ IS-IS 路由协议术语

- IS（Intermediate System），中间系统。相当于 TCP/IP 中的路由器，是 IS-IS 协议中生成路由和传播路由信息的基本单元。在下文中 IS 和路由器具有相同的含义。
- ES（End System），终端系统。相当于 TCP/IP 中的主机系统。ES 不参与 IS-IS 路由协议的处理，ISO 由专门的 ES-IS 协议定义终端系统与中间系统间的通信。
- RD（Routing Domain），路由域。在一个路由域中一群 IS 通过相同的路由协议来交换

路由信息。

- Area，区域，路由域的划分单元。
- LSDB（Link State DataBase），链路状态数据库。所有的网络内连接状态组成了链路状态数据库，在每一个 IS 中都至少有一个 LSDB。IS 使用 SPF 算法，利用 LSDB 来生成自己的路由。
- LSPDU（Link State Protocol Data Unit），链路状态协议数据单元。在 IS-IS 中，每一个 IS 都会生成一个 LSP，此 LSP 包含了本 IS 的所有链路状态信息。每个 IS 收集本区域内所有的 LSP 生成自己的 LSDB。
- NPDU（Network Protocol Data Unit），网络协议数据单元。是 ISO 中的网络层协议报文，相当于 TCP/IP 中的 IP 报文。DIS（Designated IS），广播网上的指定中间系统。
- NSAP（Network Service Access Point），网络服务接入点，即 ISO 中网络层的地址。用来标识一个抽象的网络层访问服务点，描述 ISO 模型的网络地址结构。

■ IS-IS 路由协议适用的链路类型

IS-IS 可以运行在点到点链路（Point to Point Links），如 PPP、HDLC 等，也可以运行在广播链路（Broadcast Links），如 Ethernet、Token-Ring 等，对于 NBMA（Non-Broadcast Multi-Access）网络，需对其配置子接口，并将子接口类型配置为 P2P 或广播网络。IS-IS 不能在点到多点链路（Point to Multi Point Links）上运行。

2. IS-IS 路由协议结构

为了支持大规模的路由网络，IS-IS 在路由域内采用两级的分层结构。一个大的路由域被分成一个或多个区域（Areas）。区域内的路由通过 Level-1 路由器管理，区域间的路由通过 Level-2 路由器管理。

■ Level-1 路由器

Level-1 路由器负责区域内的路由，它与同一区域的 Level-1 路由器或 Level-1-2 路由器形成邻居关系，维护一个 Level-1 的 LSDB，该 LSDB 包含本区域的路由信息，到区域外的报文转发给最近的 Level-2 路由器。

- 只与本区域的路由器形成邻居。
- 只参与本区域内的路由，只保留本区域的数据库信息。
- 通过与自己相连的 L1/2 路由器的 ATT bit 寻找与自己最近的 L1/2 路由器。
- 通过发布指向离自己最近的 L1/2 路由器的缺省路由，访问其他区域。

■ Level-2 路由器

Level-2 路由器负责区域间的路由，可以与其他区域的 Level-2 路由器或 Level-1-2 路由器形成邻居关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。所有 Level-2 路由器组成路由域的骨干网，负责在不同区域间通信，路由域中的 Level-2 路由器必须是连续的，以保证骨干网的连续性。

- 可以与其他区域的 L2 路由器形成邻居。
- 参与骨干区的路由。
- 保存整个骨干区的路由信息。

- L1/2 路由器同时可以参与 L1 路由。

■ **Level-1-2 路由器**

同时属于Level-1和Level-2的路由器称为Level-1-2路由器，每个区域至少有一个Level-1-2路由器，以将区域连在骨干网上。它维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

- 可以和本区域的任何级别路由器形成邻居关系；可以和其他域相邻的 L2 或 L1/2 路由器形成邻居关系。
- 可能有两个级别的链路状态数据库。
- L1 用来作为区域内路由，L2 用来作为区域间路由。
- 完成它所在的区域和骨干之间的路由信息的交换，将 L1 LSDB 中的路由信息转换到 L2 LSDB 中，以在骨干中传播，既承担 L1 的职责，也承担 L2 的职责。
- 通常位于区域边界上。

3. IS-IS 路由协议的特点

IS-IS 路由协议具有以下特点：

- IS-IS 是 ISO 定义的 OSI 协议栈中无连接网络服务（Connectionless Network Service，CLNS）的一部分。
- IS-IS 直接运行于链路层之上。
- IS-IS 是链路状态路由协议，维护一个链路状态数据库，并使用 SPF 算法来计算最佳路径。
- 用 Hello 包建立和维护邻居关系。
- 支持灵活的 TLV（type-length-value）编址方式，协议扩展性好。
- 使用区域来构造两级层次化的拓扑结构。
- 在区域之间可以使用路由汇总来减少路由器的负担。
- 支持 VLSM 和 CIDR。
- 在广播多路访问网络通过选举指定 IS（DIS）来管理和控制网络上的泛洪扩散。
- 具有认证功能。
- IS-IS 采用 Cost 作为度量值。
- 路由收敛速度快，结构清晰。
- 适合大型网络。

8.2.5 BGP 路由协议

BGP（Border Gateway Protocol，边界网关协议）是一种自治系统间的动态路由发现协议，是为 TCP/IP 设计的外部网关协议，用于多个自治域之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号/自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

1. BGP 协议的特点

BGP 是唯一一个用来处理超大规模互联网络的网络协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。当前使用的版本是 BGPv4（请参阅 RFC1771）。BGPv4 适用于分布式结构，并支持无类域间路由 CIDR，正迅速成为事实上的 Internet 外部路由协议标准，BGP 协议经常用于 ISP 之间。利用 BGP 还可以实施用户配置的策略。

BGP 具有以下主要特点：

- BGP 是一种外部网关协议（Exterior Gateway Protocol，EGP），与 OSPF、RIP 等内部网关协议（Interior Gateway Protocol，IGP）不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。
- 用属性（Attribute）而不是用度量值来描述路径。
- BGP 使用 TCP 作为传输层协议（端口号 179），继承了 TCP 的可靠性和面向连接的特性，并且可以通过 Keepalive 信息检验 TCP 的连接。
- BGP 支持 CIDR 和 VLSM。
- 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。
- 拥有自己的 BGP 表，BGP 路由通过携带 AS 路径信息彻底解决路由环路问题。
- BGP 提供了丰富的属性特征和路由策略，能够对路由实现灵活的过滤和选择。
- BGP 易于扩展，不仅适合在大型网络中使用，而且能够适应网络新的发展。

发送 BGP 消息的路由器称为 BGP 发言者（BGP Speaker），它接收或产生新的路由信息，并发布（Advertise）给其他 BGP 发言者。当 BGP 发言者收到来自其他自治系统的新路由时，如果该路由比当前已知路由更优、或者当前还没有该路由，它就把这条路由发布给自治系统内所有其他 BGP 发言者。

相互交换消息的 BGP 发言者之间互称对等体（Peer），若干相关的对等体可以构成对等体组（Peer group）。

尽管 BGP 协议是为自治系统间的路由选择而设计，但它也可以用于自治系统内部，是一类双重路由选择协议。两个可以在自治系统之间进行通信的 BGP 相邻结点必须存在于同一个物理链路上。位于同一个自治系统内的 BGP 路由器可以互相通信，以确保它们对整个自治系统的所有信息都相同，而且通过信息交换后，它们将决定自治系统内哪个 BGP 路由器作为连接点来负责接收来自自治系统外部的信息。

BGP 在路由器上以下列两种方式运行：

- IBGP（Internal BGP）：当 BGP 运行于同一自治系统内部时，被称为 IBGP。
- EBGP（External BGP）：当 BGP 运行于不同自治系统之间时，称为 EBGP。

2. BGP 路由选择规则

■ BGP 选择路由的策略

在目前的实现中，BGP 选择路由时采取如下策略：

- 首先丢弃下一跳（NEXT_HOP）不可达的路由；
- 优选 Preferred-value 值最大的路由；
- 优选本地优先级（LOCAL_PREF）最高的路由；

- 优选聚合路由；
- 优选 AS 路径（AS_PATH）最短的路由；
- 依次选择 ORIGIN 类型为 IGP、EGP、Incomplete 的路由；
- 优选 MED 值最低的路由；
- 依次选择从 EBGP、联盟、IBGP 学来的路由；
- 优选下一跳 Cost 值最低的路由；
- 优选 CLUSTER_LIST 长度最短的路由；
- 优选 ORIGINATOR_ID 最小的路由；
- 优选 Router ID 最小的路由器发布的路由；
- 优选地址最小的对等体发布的路由。

■ **BGP 负载分担的路由选择**

在 BGP 中，由于协议本身的特殊性，它产生的路由的下一跳地址可能不是当前路由器直接相连的邻居。常见的一个原因是 IBGP 之间发布路由信息时不改变下一跳。这种情况下，为了能够将报文正确转发出去，路由器必须先找到一个直接可达的地址（查找 IGP 建立的路由表项），通过这个地址到达路由表中指示的下一跳。在上述过程中，去往直接可达地址的路由被称为依赖路由，BGP 路由依赖于这些路由指导报文转发。根据下一跳地址找到依赖路由的过程就是路由迭代（recursion）。

目前系统支持基于迭代的 BGP 负载分担，即如果依赖路由本身是负载分担的（假设有三个下一跳地址），则 BGP 也会生成相同数量的下一跳地址来指导报文转发。需要说明的是，基于迭代的 BGP 负载分担在系统上始终启用。

在实现方法上，BGP 的负载分担与 IGP 的负载分担有所不同：

- IGP 是通过协议定义的路由算法，对到达同一目的地址的不同路由，根据计算结果，将度量值（metric）相等的（如 RIP、OSPF）路由进行负载分担，选择的标准很明确（按 metric）。
- BGP 本身并没有路由计算的算法，它只是一个选路的路由协议，因此，不能根据一个明确的度量值决定是否对路由进行负载分担，但 BGP 有丰富的选路规则，可以在对路由进行一定的选择后，有条件地进行负载分担，也就是将负载分担加入到 BGP 的选路规则中去。

■ **BGP 发布路由的策略**

在目前的实现中，BGP 发布路由时采用如下策略：

- 存在多条有效路由时，BGP 发言者只将最优路由发布给对等体；
- BGP 发言者只把自己使用的路由发布给对等体；
- BGP 发言者从 EBGP 获得的路由会向它所有 BGP 对等体发布（包括 EBGP 对等体和 IBGP 对等体）；
- BGP 发言者从 IBGP 获得的路由不向它的 IBGP 对等体发布；
- BGP 发言者从 IBGP 获得的路由发布给它的 EBGP 对等体（关闭 BGP 与 IGP 同步的情况下，IBGP 路由被直接发布；开启 BGP 与 IGP 同步的情况下，该 IBGP 路由只有在 IGP 也发布了这条路由时才会被同步并发布给 EBGP 对等体）；
- 连接一旦建立，BGP 发言者将把自己所有的 BGP 路由发布给新对等体。

第 9 章　路由器的选择与适用

路由器是构成 IP 网络的核心，其最基本的作用就是连接不同类型的网络，智能选择最佳的信息传送线路。除此以外，路由器还具有访问控制功能。路由器也可以算作是一台专用计算机，而它的价格之所以昂贵，就在于其功能强大的软件——IOS（Internet Operation System，因特网操作系统），可以听懂并翻译各种网络协议，就像一个会讲各种语言的人一样。

9.1　路由器的分类

路由器的主要功能和一般应用虽然没有明显区别，但是为了满足各种应用需求，也出现过各式各样的路由器，无论是在价格还是在产品性能方面都存在着很大的差异。路由器的分类标准也不是唯一的，根据不同的标准，可以对路由器作不同的分类。

9.1.1　按性能划分

从路由性能上，路由器可分高端、中端、低端和 SOHO 路由器。

SOHO 路由器主要适用于 SOHO 网络的 Internet 接入，通常采用固定配置路由器。Cisco 800/500 系列路由器（如图 9-1 所示）即属于 SOHO 路由器，集成了因特网接入、安全和无线服务。

图 9-1　Cisco 800/500 系列路由器

低端路由器主要适用于中小型网络的 Internet 接入或企业分支机构网络远程接入，端口数量和类型、包处理能力都非常有限。Cisco 1800/2800 系列、Cisco 1900/2900 系列属低端路由器，Cisco 3800 系列、Cisco 3900 系列和 Cisco 4400 系列属中低端路由器。图 9-2 所示为 Cisco 3900 系列路由器。

中端路由器适用于较大规模的网络，拥有较高的包处理能力，具有较丰富的网络接口，适应较为复杂的网络结构。Cisco 7200/7600 系列属于中高端路由器，作为可扩展的多用途系统，能够为大中型网络应用提供可靠的第二层和第三层服务，可用于构建企业级数据中心互连平台。图 9-3 所示为 Cisco 7609 路由器。

图 9-2 Cisco 3900 系列中低端路由器

图 9-3 Cisco 7609 中高端路由器

高端路由器主要应用于大型网络的核心路由器，拥有非常高的包处理性能，并且端口密度高、端口类型多，以适应复杂的网络环境。Cisco ASR 1000/9000 和 XR 12000 系列属高端路由器，多被电信级运营商用于构建超大规模的分布式结构网络。图 9-4 所示为 Cisco ASR 9000 系列路由器。

图 9-4 Cisco ASR 9000 系列高端路由器

Cisco 1900/2900/3900/4400 系列路由器为 ISR G2 路由器，无论是硬件配置还是功能支持，都比 ISR 路由器有了较大幅度的提升（如表 9-1 所示）。

表 9-1 ISR 与 ISR G2 比较

	集成多业务路由器（ISR）	第二代集成多业务路由器（ISR G2）
广域网性能	处理服务时最大传输速率 45 Mbps	处理服务时最大传输速率 150 Mbps
网络处理器	单核处理器	多核处理器，支持未来扩展
服务模块性能和容量	1X 倍速和 160 GB 存储容量	双核处理器最高支持 7X 倍速；1 TB 存储容量
板载 DSP	仅话音	话音和视频就绪 DSP
交换机模块	支持以太网供电 (PoE) 的快速以太网	支持以太网供电（PoE）的快速以太网/千兆位以太网
IOS 镜像	多个镜像	仅一个通用 IOS 镜像
服务交付	硬件耦合	随需应变的服务
冗余	单主板	可现场更换的主板
能效	EnergyWise	EnergyWise 搭配基于插槽的控件

9.1.2 按结构划分

从结构上分，路由器可分为模块化结构与非模块化结构。通常情况下，几乎所有的中高低端路由器均为模块化结构，可以使用各种类型的模块灵活配置路由器，增加端口的数量、提供丰富的端口类型，以适应企业不断变化的业务需求。如图 9-5 所示为 Cisco 3640 模块化路由器。

图 9-5　Cisco 3640 模块化路由器

SOHO 路由器多为非模块化结构，只能提供固定类型和数量的端口。如图 9-6 所示为应用于 SOHO 的 Cisco SOHO 90 固定配置路由器。

图 9-6　Cisco SOHO 90 固定配置路由器

9.1.3 按网络位置划分

从路由器在网络中所处的位置划分，可以分为核心路由器、分发路由器和接入路由器（如图 9-7 所示）。

核心路由器位于数据网络中心，通常选用性能稳定的中高端模块化路由器。要求快速的包转发能力与高速的网络接口，全部为大容量、高性能的模块化结构。

分发路由器主要用于实现接入路由器的汇接与转发，并接入核心路由器。主要目标是以尽量便宜的方法实现尽可能多的端点互连，并且进一步要求支持不同的服务质量。分发路由器主要采用中低端路由器，主要特点就是端口数量多、价格便宜、应用简单。

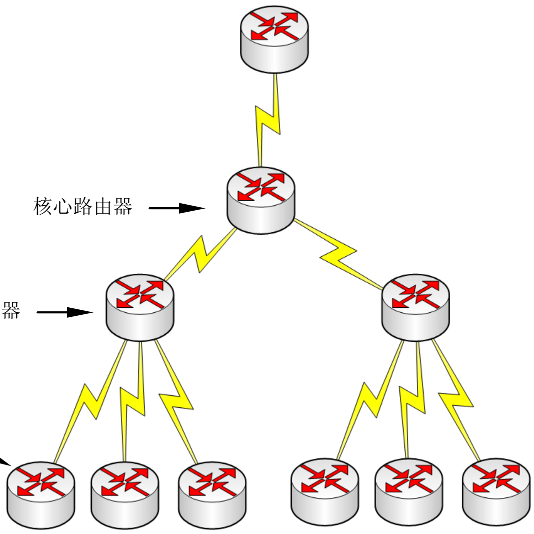


图 9-7　不同网络位置的路由器

接入路由器一般位于网络边缘，也可以称为“边缘路由器”，通常使用中低端产品，也是目前应用最广泛的一类路由器，主要应用于中小型企业或大型企业的分支机构中，要求相对低速的端口及较强的接入控制能力。

9.1.4 按功能划分

从路由器的功能方面划分，路由器可分为通用路由器与专用路由器。一般所说的路由器为通用路由器。专用路由器通常为实现某种特定功能对路由器接口、硬件等作专门优化，如网吧路由器、安全路由器、VPN 路由器等。例如，侠诺 QNO 网吧专用路由器（如图 9-8 所示），适合大量用户同时进行在线网络游戏、视频聊天、网上电影等应用；带宽汇聚既可节约费用，又能避免带宽不足的问题；强效防火墙具备 ARP 攻击防御能力，保证网络更加安全。

图 9-8　网吧专用路由器

9.1.5 按转发性能划分

从数据转发性能上分，路由器可分为线速路由器和非线速路由器。通常线速路由器是高端路由器，能以物理链路所支持的最高速率转发数据包；中低端路由器大多是非线速路由器，只能以低于线速的速率转发数据。

9.1.6 按网络类型划分

从广义的角度而言，路由器可分为有线路由器和无线路由器两大类。顾名思义，有线路

由器就是借助物理连线（光纤、双绞线、同轴电缆等）建立连接的路由器。常见的（或者说传统的）路由器基本上都是有线路由器。无线路由器是随着无线网络应用的快速普及，在近几年才出现的新产品。无线路由器的功能和有线路由器没有什么区别，同样是用来连接不同的网络或 Internet 接入，不同的是它的连接不是通过有形的连线实现的，而是借助无形的电磁波实现的。图 9-9 所示为支持无线网络连接的 Cisco 1900 无线路由器。

图 9-9　Cisco 1900 无线路由器

当然，无线路由器除了提供无线接口以外，也提供有线连接端口（以固定端口方式提供，或者借助相应的网络模块提供）。一些中低端路由器通过安装无线路由模块，也可以提供对无线网络的支持。图 9-10 所示为 Cisco 中低端路由器的无线局域网模块。

图 9-10　中低端路由器的无线局域网模块

9.2　路由器的参数

如今的路由器市场真可谓百家争鸣，不同类型的产品其功能和应用领域也会有所不同，那么如何才能根据自己的网络规模选择一款合适的路由器呢，在选择路由器时，应当考虑哪些因素和参数呢？

9.2.1　路由器基本参数

■　接口类型

路由器能支持的接口类型，体现了路由器的通用性。常见的接口类型有：通用串行接口（如 RS 232 DTE/DCE 接口、V.35 DTE/DCE 接口、X.21 DTE/DCE 接口、RS 449 DTE/DCE 接口和 EIA530 DTE 接口等），10 Mbps、10/100 Mbps、1000 Mbps 以太网接口，GBIC 插槽、SFP 插槽和 ATM 接口等。对于模块化路由器而言，业务板类型是否齐全，决定着接口类型是否丰富。图 9-11 所示为拥有丰富接口类型的各种业务板。

■ **CPU**

对于任何一款路由器产品，CPU 都是它的“大脑”。通常在中低端路由器中，CPU 负责交换路由信息、路由表查找，以及转发数据包。CPU 的能力直接影响路由器的吞吐量（路由表查找时间）和路由计算能力（影响网络路由收敛时间）。在高端路由器中，通常包转发和查表功能由 ASIC 芯片完成，CPU 只实现路由协议、计算路由，以及分发路由表等任务。由于技术的发展，路由器中许多工作都可以由硬件实现（专用芯片）。CPU 性能并不完全反映路由器的性能。路由器性能由路由器吞吐量、时延和路由计算能力等指标体现。图 9-12 所示为 Intel IXP 2350 网络处理器。

图 9-11　拥有丰富接口类型的各种业务板

图 9-12　Intel IXP 2350 网络处理器

■ **内存**

路由器中可能有多种内存（如图 9-13 所示），例如闪存（Flash）、DRAM 等。内存用于存储配置、路由器操作系统、路由协议软件等。在中低端路由器中，路由表可能存储在内存中。通常来说路由器内存越大越好（不考虑价格）。但是，与 CPU 能力类似，内存同样不直接反映路由器的性能。因为高效的算法与优秀的软件可能大大节约内存。

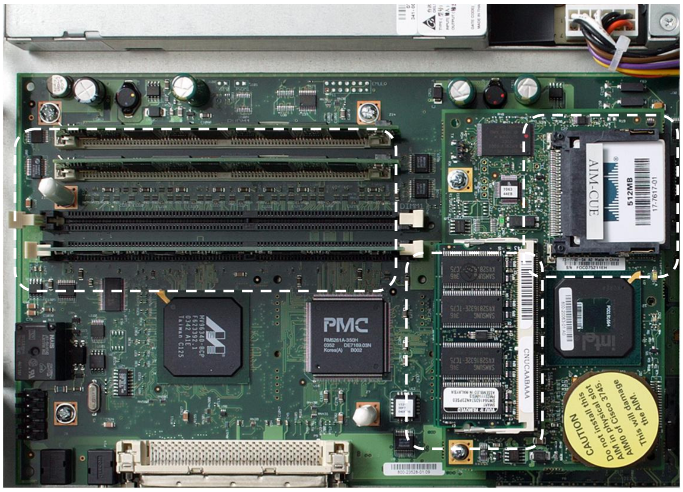


图 9-13　内存

为了便于配置和系统升级，许多路由器外置了 Flash 插槽，可以根据需要选择相应容量的闪存卡。图 9-14 所示为路由器管理模块与闪存卡。

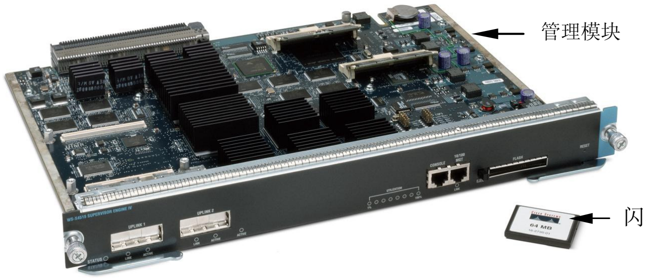


图 9-14　路由器管理模块和内存卡

■　**背板能力**

背板能力，是指路由器背板容量或者总线带宽能力，体现于路由器的吞吐量。背板能力对于保证整个网络之间的连接速度是非常重要的。如果所连接的两个网络速率都较快，而由于路由器的带宽限制，这将直接影响整个网络之间的通信速度。所以，对于连接较大网络的中高端路由器而言，当网络间的数据流量较大时，应当特别关注路由器的背板容量、背板能力。

■　**端口吞吐量**

端口吞吐量，是指路由器包转发能力，即路由器在某端口上的包转发能力，基本可以衡量路由器的路由性能。以 pps（包每秒）为单位，应当达到线速处理能力。端口吞吐量通常采用两个相同速率接口测试。但是，测试接口可能与接口位置及关系相关。例如，同一插卡上端口间测试的吞吐量，可能与不同插卡上端口间吞吐量值不同。

提·示　中高端路由器可以对较大的数据包进行正确快速转发；而低端路由器则只能转发小的数据包，对于那些较大的数据包，则需要拆分成许多小的数据包来分开转发，数据包的转发能力就差了。其实，这与背板容量有非常紧密的关系。

■　**丢包率**

丢包率，是指路由器在稳定的持续负荷下，由于资源缺少在应该转发的数据包中不能转发的数据包所占的比例。丢包率的大小会影响到路由器线路的实际工作速度，严重时甚至会使线路中断。

提·示　小型企业网络一般流量不会很大，所以出现丢包现象的机会也很小。因此，低端路由器对该参数不必作太多考虑。

■　**转发时延**

转发时延，是指需转发的数据包最后一比特进入路由器端口，到该数据包第一比特出现在端口链路上的时间间隔。转发时延较高时，不仅会影响网络传输效率，而且还不能很好地实现视频会议、IP 电话等实时通信。该参数与背板容量、吞吐量等参数紧密相关。

■ **路由表能力**

路由器通常依靠建立及维护的路由表来决定如何转发。路由表能力，是指表内所容纳路由表项数量的极限。一般来说，高端路由器路由表容量应当较大，因为它将面对非常庞大的网络，而中低端路由器通常对路由表能力没有什么要求。原因很简单，其所应用的网络结构相对简单。该参数与路由器自身所带的缓存大小有关。

■ **网络协议**

路由器应当支持开放标准的协议。开放标准的协议是设备互连的良好前提，所支持的协议也意味着设计上的灵活和高效。例如，是否支持完全的组播路由协议、是否支持 MPLS、是否支持冗余路由协议 VRRP。此外，如果网络有特殊需求，那么在考虑 TCP/IP 路由的同时，还应当考虑路由器对其他路由协议的支持能力。

一些设备厂商为了提高效率，会开发出一些私有的协议，用户在选择这些特性上最好根据自己的需要选择，同时应当尽量避免在核心技术上采用此类技术。原因很简单，不标准的协议意味着不同设备供应商之间的不兼容，从而使用户困死在一个设备供应商上。同时，不标准的协议在历史上也往往是被新型的开放协议所取代。

■ **可靠性**

可靠性，是指路由器的可用性、负载承受能力、无故障工作时间和故障恢复时间等指标。路由器的可靠性主要体现在接口故障和网络流量增大时的适应能力，保证这种适应能力的方式就是备份。可靠性也是选择路由器应该考虑最多的问题，因为路由器的安全可靠实际上就是网络安全可靠的保障。可靠性也包括多个方面，如硬件冗余、模块热插拔等。

> **提·示** 可靠性通常是由用户口碑、品牌信誉、产品销量、技术先进等作为保障的。

■ **安全性**

由于网络黑客和病毒的流行，设备本身的保护和抵御能力也是选择路由器的一个重要因素。已经有部分路由器提供了防止黑客攻击的手段，提供设备安全连接 SSH 和安全复制（SCP）功能。另外，路由器本身在使用 RADIUS/TACACS+等认证的同时，会使用大量的访问控制列表（ACL）来屏蔽和隔离病毒，因此在选择路由器时应注意 ACL 的控制方式。如果采用 CPU 检查方式，将会降低路由器的运行性能，而采用硬件实现的方式，则不会对运行构成额外的负担。

■ **可管理性**

路由器设备可管理性代表了设备监控、维护和管理的重要特性。用户在选择时也必须考虑到设备厂商所能提供的网管系统、对设备本身可管理的方式和方法。

■ **其他功能**

路由器除了应当具备传统的数据传输、包交换功能之外，还要支持数据分类、优先级控制、用户识别和快速自愈等特性。具体来讲，VPN、QoS 能力、组播技术、安全和管理性都要具备。同时，随着语音应用的发展，是否支持语音功能也要视自己的应用情况来决定。Cisco

的集成多业务路由器（简称 ISR），可实现集成语音、安全、视频、无线等主要应用，为中小型企业、大型企业分支机构提供安全、线速的数据、话音、视频和其他高级服务。既满足了客户分支机构更安全地快速访问公司内部数据资源，同时还可以通过选装模块获得诸如 VPN 加速、增强的入侵防护、URL 过滤、话音交换系统等增强性网络服务。

9.2.2 路由器性能参数

路由器性能参数主要包括以下几个方面。

■ **全双工线速转发能力**

路由器最基本且最重要的功能是数据包转发。在同样端口速率下转发小包是对路由器包转发能力最大的考验。全双工线速转发能力是指以最小包长（以太网 64 B、POS 口 40 B）和最小包间隔（符合协议规定）在路由器端口上双向传输的同时不引起丢包。该指标是路由器性能的重要指标。

■ **设备吞吐量**

指设备整机包转发能力，是设备性能的重要指标。路由器的工作在于根据 IP 包头或者 MPLS 标记选路，所以性能指标是每秒转发的包数量。设备吞吐量通常小于路由器所有端口吞吐量之和。

■ **端口吞吐量**

端口吞吐量是指端口包转发能力，通常使用：PPS（包每秒）来衡量，它是路由器在某端口上的包转发能力。通常采用两个相同速率接口测试。但是测试接口可能与接口位置及关系相关。例如同一插卡上端口间测试的吞吐量可能与不同插卡上端口间的吞吐量值不同。

■ **背靠背帧数**

背靠背帧数是指以最小帧间隔发送最多数据包不引起丢包时的数据包数量。该指标用于测试路由器缓存能力。有线速全双工转发能力的路由器该指标值无限大。

■ **路由表能力**

路由器通常依靠所建立及维护的路由表来决定如何转发数据。路由表能力是指路由表内所容纳路由表项数量的极限。由于 Internet 上执行 BGP 协议的路由器通常拥有数十万条路由表项，所以该项目也是路由器能力的重要体现。

■ **背板能力**

背板能力是路由器的内部实现。背板能力体现在路由器的吞吐量上：背板能力通常大于依据吞吐量和测试包场所计算的值。但是背板能力只能在设计中体现，一般无法测试。

■ **丢包率**

丢包率是指测试中所丢失数据包数量占所发送数据包的比率，通常在吞吐量范围内测试。丢包率与数据包长度及包发送频率相关。在一些环境下可以加上路由抖动、大量路由后测试。

■ **时延**

时延是指数据包第一个比特进入路由器到最后一个比特从路由器输出的时间间隔。在测

试中通常使用测试仪表发出测试包到收到数据包的时间间隔。时延与数据包长相关，通常在路由器端口吞吐量范围内测试，超过吞吐量测试该指标没有意义。

■ **时延抖动**

时延抖动是指时延变化。数据业务对时延抖动不敏感，所以该指标没有出现在 Benchmarking 测试中。由于 IP 上的多业务，包括语音、视频业务的出现，该指标才有测试的必要性。

■ **VPN 支持能力**

通常路由器都能支持 VPN。其性能差别一般体现在所支持的 VPN 数量上。专用路由器一般支持的 VPN 数量较多。无故障工作时间，该指标按照统计方式指出设备无故障工作的时间。一般无法测试，可以通过主要器件的无故障工作时间计算或者大量相同设备的工作情况计算。

■ **内部时钟精度**

拥有 ATM 端口做电路仿真或者 POS 口的路由器互连通常需要同步。如使用内部时钟则其精度会影响误码率。内部时钟精度级别定义及测试方法可参见相应同步标准。

9.3 路由器的选择策略

在组建局域网时，路由器的选择也是一项重要的内容。在选购时，要根据用户的实际使用情况，首先确定是选择接入级、骨干级还是企业级路由器，然后再根据路由器选择方面的基本原则，确定产品的基本性能要求。

9.3.1 路由器的选购原则

选购路由器时，应当遵循以下基本原则。

● 协议标准化原则

必须选择基于国际标准或行业标准的路由器。由于一些特殊路由协议，只有特定厂商的产品才予以支持，因此不太适合充当大型广域网络中的路由设备。

● 操作简单化原则

必须选择技术实用、操作简单的路由器。实现的技术越简单，包处理效率越高、越不容易发生故障。操作过程越简单，实现功能的配置和管理就越方便。同一系列产品的路由器操作系统应当与交换机操作系统完全一致或基本一致，从而减轻网络管理员学习和掌握相关技术的难度。例如，不仅所有 Cisco 网络设备（如交换机、路由器、防火墙甚至无线设备）都采用 Cisco IOS 操作系统，而且许多业务模块都可以互用。同时，不仅路由器系列、交换机系列的模块可以通用，而且路由器和交换机的模块也可以通用。除此之外，Cisco 还分别为交换机、路由器和安全设备提供了图形化配置和管理界面，实现了网络设备的傻瓜化管理。

● 环境适应化原则

必须选择环境适应性强的路由器。如果网络规模较大，网络链路形式复杂，网络应用多样，那么将要求路由器拥有较高的适应能力。同时，路由器还应当具有一定的可扩展性，能够适应网络规模的扩大，或者拓扑结构的改变。也就是说，不仅要提供种类丰富的端口，以满足

与远程路由设备的连接，而且还应当提供丰富的功能，从而实现网络应用所需要的各种服务。

- 设备可管理原则

必须选择拥有强大监管和配置能力的路由器。路由器应当能够提供丰富的系统统计信息和运行日志，能够实现对故障的诊断和追踪，实现对深层故障的检测诊断，并能有效地实现设备的远程管理和维护，甚至在故障发生前或故障发生时，及时向网络管理员发出警告。

- 系统容错冗余原则

用户在选择路由器时，应充分考虑设备是否支持热插拔，支持备份设置，支持自动切换等功能。对于大型网络中关键应用的核心路由器，应当拥有冗余电源、冗余风扇等模块。图 9-15 所示为 Cisco 7613 高可用性路由器，拥有 2 个冗余管理模块，以及 2 个冗余电源模块。

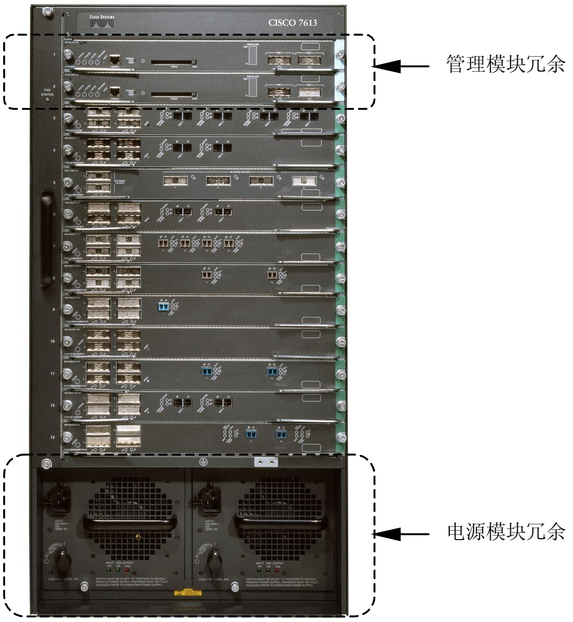


图 9-15　Cisco 7613 高可用性路由器

- 安全可靠性原则

针对现代网络存在的各种安全隐患，路由器必须具有可靠的安全特性。路由器系统软件本身应当具有简单的 IDS 和 IPS 功能，拥有抵御一般网络攻击的能力，从而保护内部网络不受外部恶意攻击的侵害。当然，如果能够配置相应的功能模块，其安全效果将会更加完美。图 9-16 所示为应用于 Cisco 路由器的防火墙模块，可以让路由器所有端口都充当防火墙端口。

图 9-16　Cisco 路由器的防火墙模块

9.3.2 选购时应考虑的因素

在选购路由器时，还应当认真考虑以下因素。

- 实际需求

作为电子产品，网络技术成熟周期不断缩短、设备制造成本不断下降、网络需求和网络应用日新月异，因此网络设备的淘汰周期（通常为5年左右）也在不断加快。所以，在制订设备购置计划时，应当考虑网络规模和网络应用的实际需要，不要盲目追求高性能、高稳定性，只要能满足实际需求并略有性能储备就可以了。

- 可扩展性

充分考虑到近期内（1～3 年内）可能的网络扩展和升级，路由设备（尤其是核心路由设备）的性能和插槽都应当留有一定的扩展余地，以适应网络拓扑结构变化、网络应用服务发展、网络数据传输量增加的需要。

- 性能和稳定性

兼顾产品的性能和稳定性，既保证网络数据的高速传输，又保障网络链路的稳定传输，还拥有丰富的功能和充分的安全性。总之，对于作为网络核心（利用路由设备作为核心设备）和网络边界（利用路由器实现与其他网络的连接）的路由器而言，高速、高效、稳定、安全两者缺一不可。

- 产品性价比

无论是企事业单位，还是政府机关，在能够满足网络对性能和稳定性要求的前提下，应当尽量压缩开支，选择价格低廉、最具性价比的路由产品。近几年，国内网络设备厂商（如华为、锐捷）的技术不断成熟，设备的整体性能已经达到和接近国外知名产品的水平。因此，在性能相近的情况下，建议选择更具价格优势、更加安全的国货产品。

提·示　对于大专院校和教育科研部门而言，如果采购进口产品，还可以申请享有免增值税和关税，从而节约大致20%的费用。

- 产品品牌

品牌往往是技术含量和稳定性的保障，因此选择路由器时，不可避免地将涉及品牌因素的影响。通常情况下，应选择知名品牌的产品。另外，路由器和交换机应当尽量选择同一厂商的产品，以保证设备之间的连通性和兼容性，以及网络协议和网络技术的一致性。

另外，品牌往往与服务连接在一起。路由器作为一种高科技产品，售前售后的支持和服务显得尤其重要。应尽量选择售后服务方便、快捷的产品。

第 10 章　路由器的接口与连接

当需要将局域网接入 Internet、实现远程网络互连时，就必须借助于路由器。路由器的硬件连接包括与局域网设备之间的连接、与广域网设备之间的连接。路由器的接口类型也非常丰富，用于实现与不同类型网络的连接。

10.1　路由器模块和接口卡

由于路由器大多为模块化配置，因此，除少量由机箱直接提供的固定端口外，其他大多数类型的端口（尤其是广域网端口）都是由路由器扩展模块提供的。因此，在应用中要根据网络连接和网络链路的实际需求选择相应的模块，以便提供所需接口。

10.1.1　SPE

SPE（Services Performance Engine，业务性能引擎）是模块化主板，可使用未来开发的更高性能的引擎升级。自 Cisco 3900 系列路由器开始，可以实现现场可更换业务性能引擎，并随网络和分支机构需求的发展而扩展路由器性能。图 10-1 所示为 Cisco SPE 业务性能引擎。

图 10-1　SPE 业务性能引擎

10.1.2　SM/SM-X

服务模块（Service Module，SM）始于 Cisco 2800/3800 系列提供，每个服务模块插槽均提供高数据吞吐功能，到路由处理器的聚合吞吐量可达 4 Gbps 聚合，通过 MGF 到其他模块插槽的聚合吞吐量可达 2 Gbps。

增强型服务模块（Enhanced Services Module，SM-X）始于 Cisco 4400 系列提供，每个服务模块插槽可以向路由处理器和其他模块插槽提供高达 10 Gbps 的高速数据吞吐能力。

SM/SM-X 插槽高度灵活，除支持半宽服务模块外，还支持双宽度服务模块（SM-Ds），即需要两个 SM 插槽的服务模块，为较高密度模块提供灵活性。服务模块插槽可提供相对于网络模块插槽两倍的电源功能，从而允许具有较高可扩展性和较佳性能模块的灵活性。

SM-X 可利用服务模块插槽中支持网络接口模块的承载卡，增加端口密度。

SM/SM-X 插槽支持在线插拔（Online Insertion and Removal，OIR），在需要新增或更换模块时，不必停机，从而可以有效地减少宕机时间。

另外，SM/SM-X 插槽可用来替换用于语音/传真（EVM）的网络模块插槽和扩展模块插槽。适配器模块支持与现有网络模块、增强的网络模块（NME）以及 EVM 的后向兼容性。图 10-2 所示为增强型以太网交换 SM 模块（Enhanced EtherSwitch Service Module）。

图 10-2　增强型以太网交换 SM 模块

10.1.3 WIC/HWIC/EHWIC

WIC（WAN Interface Cards，广域网接口卡）插槽用于安装广域网接口模块，以提供各种类型的广域网接口。图 10-3 所示为 WIC 模块和插槽。

图 10-3　WIC 模块和插槽

HWIC（High-speed WAN Interface Cards，高速广域网接口卡）是 WIC 的升级和增强版本。HWIC 提供了高于当前 WIC 的速度和端口密度。HWIC 插槽可支持基于思科产品的馈线电源和 PoE 的模块。HWIC 有两种形式，即占一个插槽的单宽接口卡和占两个插槽的双宽接口卡。

通过拆除两个 HWIC 插槽间的中央导轨，可以将其整合为一个大型插槽（HWIC-D）。HWIC 提供嵌入式硬件加密加速，支持语音和视频的数字信号处理器（DSP，Digital Signal Processor）插槽，可选防火墙、入侵预防、呼叫处理、语音信箱，以及应用程序服务。HWIC 插槽中支持 WIC、VWIC 和 VIC。图 10-4 所示为 Cisco HWIC 模块和插槽。

图 10-4　Cisco HWIC 模块和插槽

EHWIC（Enhanced High-speed WAN Interface Cards，增强型高速广域网接口卡）插槽用于替换高速广域网接口卡（HWIC）插槽，可本地支持 HWIC、广域网接口卡（WIC）、语音接口卡（VIC），以及语音/广域网接口卡（VWIC）。图 10-5 所示为 Cisco EHWIC 4ESGP 模块，提供 4 个 1000Base-T 接口。

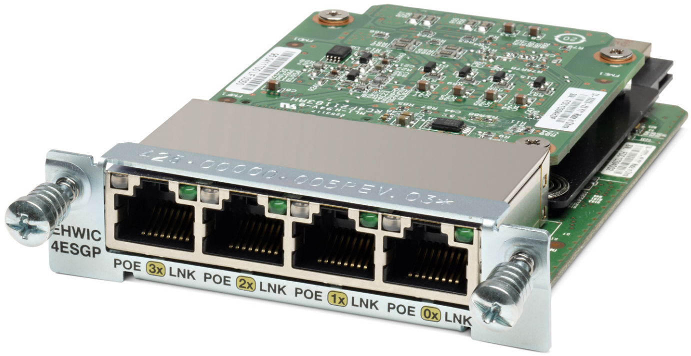


图 10-5　Cisco EHWIC 4ESGP 模块

NIM（Network Interface Modules，网络接口模块）不断发展增强型高速广域网接口卡（EHWIC），增加端口密度和模块功能。每个 NIM 插槽向路由处理器和其他模块插槽提供高达 2 Gbps 的高数据吞吐功能。NIM 支持 OIR，可减少新模块和替换模块所需的停机时间。专业 NIM 支持固态驱动器（SSD）和硬盘驱动器（HDD）。

10.1.4 PVDM/PVDM2/PVDM3/PVDM4s

PVDM（Packet Voice DSP Module，分组语音数据模块）是分组语音 DSP（Digital Signal Processor，数字信号处理器）处理模块，用于向系统提供数字信号处理资源。一般情况下，将模拟语音经采样转成原始的数字信号后，需要专用的 DSP 来将按照一定的编码来进行处理。一个 PVDM 模块由一个或多个 DSP 构成，可以执行压缩、语音活动检测、抖动管理和回声消除等功能。图 10-6 所示为 PVDM 模块与其适用的路由器。

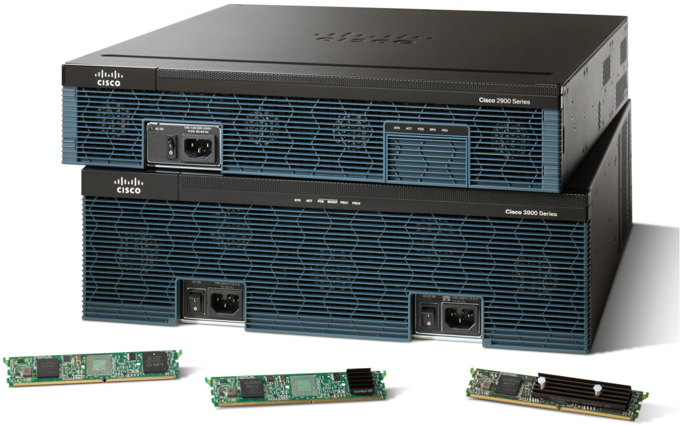


图 10-6　PVDM 模块与路由器

PVDM2 和 PVDM3 是 PVDM 的升级产品，并且能够向后兼容。PVDM3 插槽本地支持 PVDM3 模块，为多媒体语音和视频提供更高密度支持。每个 PVDM3 插槽均通过 MGF 经由 2 Gbps 聚合链路连接回系统架构。PVDM2 模块的投资保护通过适配器模块支持。PVDM 插槽的电源可通过扩展（类似于 Cisco EnergyWise 框架）管理，因此，可降低网络基础设施的能耗。未来软件版本中将提供全面的 EnergyWise 支持。

集成服务（Integrated Services Card，ISC）卡插槽支持新的 PVDM4s（High-Density Packet Voice Digital Signal Processor Modules，高密度分组语音数字信号处理器模块），用于提供大密度类型丰富的语音服务。每个 ISC 插槽都通过一个 2 Gbps 链路连接至系统构架。可在 ISC 插槽上托管未来的模块，从而改善系统功能和性能。

10.1.5　AIM/ISM

AIM（Advanced Integration Module，高级集成模块）是可插入到 Cisco 1800、Cisco 2800、Cisco 3800、Cisco 2600 和 Cisco 3700 系列路由器的内部 AIM 插槽的高级集成模块。AIM 插槽提供了一种不必降低思科平台的 LAN 或 WAN 密度，即可集成更多功能并将处理器密集型功能从主 CPU 卸载的方式，不必再占用一个外部模块化插槽。图 10-7 所示为 Cisco AIM 模块。

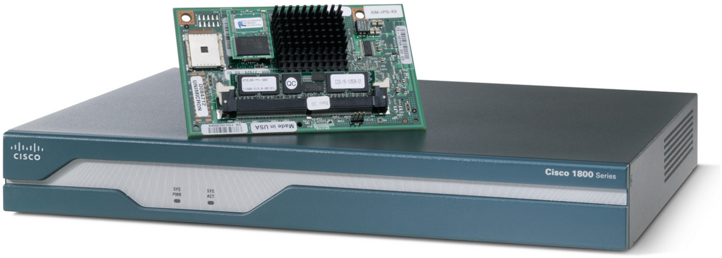


图 10-7　Cisco AIM 模块

ISM（Internal Services Module，内部业务模块）用于替换原有的 AIM 插槽，单个 ISM 插槽提供集成不需要接口端口的智能服务模块的灵活性。图 10-8 所示为 ISM 模块。

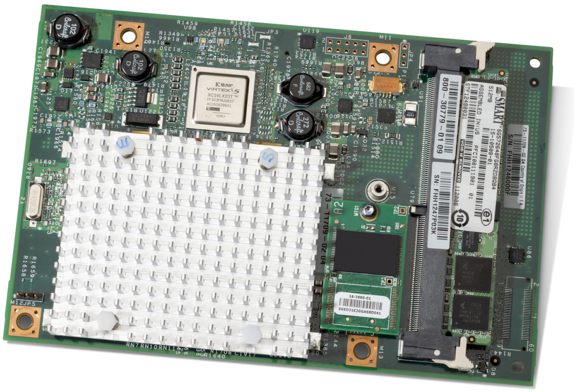


图 10-8　ISM 模块

ISM 插槽具有以下特点。

- 每个 ISM 插槽均提供高数据吞吐量功能。高达 4 Gbps 聚合到路由处理器，高达 2 Gbps 通过 MGF（MultiGigabit Fabric）聚合到其他模块插槽。
- ISM 插槽中不支持现有 AIM 模块。
- ISM 插槽的电源可通过扩展（类似于 Cisco EnergyWise 框架）管理。因此，在部署时可以降低网络基础设施的能耗。

10.1.6 NM/NME

NM（Network Module，网络模块）用于安装网络模块，提供网络接口。图 10-9 所示为 Cisco NM 模块与插槽。

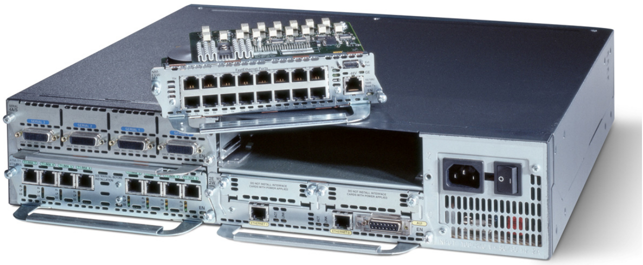


图 10-9　Cisco NM 模块

NME（Network Module Enhanced，增强网络模块）始于 Cisco 2800/3800 系列路由器的网络模块插槽，提供了比 NM 更高的性能和密度。NME 插槽连接到一条更快的 PCI 总线，以实现更高吞吐量和性能。NME 插槽也可为模块提供更高功率，以增加服务模块和模块上的密度。虽然可以在 NME 插槽中使用当前的网络模块和 WIC，但是，不能使用全部的 NME 特性。

NME 有 3 种形式，即单宽（NME，增强网络模块）、超宽（NME-X，增强扩展网络模块）和超双宽（NME-XD，高密度扩展模块），让用户可灵活地安装适合本地需求的特定密度的模块。两个紧邻的 NME 插槽可结合起来，容纳一个双宽网络模块（NMD），或双宽增强扩展网络模块（NME-XD）。图 10-10 所示为单宽 NME 模块。

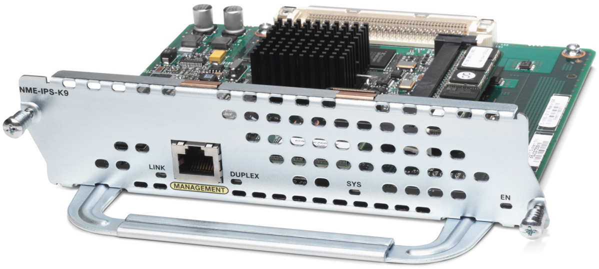


图 10-10　单宽 NME 模块

10.1.7 VIC/VWIC/EVM

VIC（Voice Interface Card，语音接口卡）用于提供语音和传真接口。图 10-11 所示为 Cisco VIC 模块。

VWIC（Voice/WAN Interface Card，语音/广域网接口卡）既可仅用于数据，也可以用于渠道化（丢弃与插入）的语音/数据综合应用，来连接 PBX（专用分组交换网）或者 PSTN（公共电话网），WIC 与 VWIC 是用户广域网连接的主要选择。图 10-12 所示为 Cisco VWIC 模块。

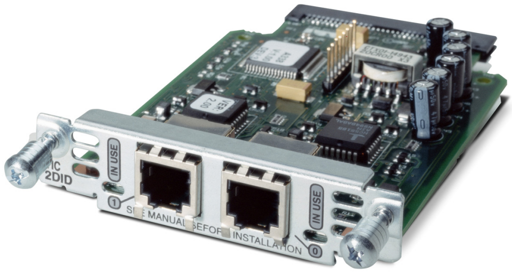


图 10-11　Cisco VIC 模块

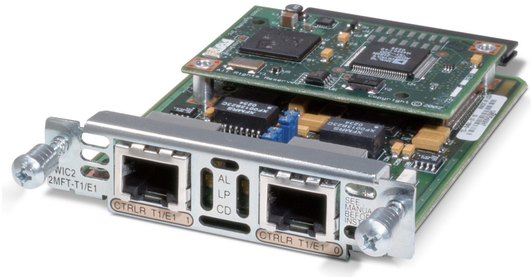


图 10-12　Cisco VWIC 模块

EVM（Extension Module for Voice/Fax）作为新型语音扩展插槽，可以提高时分多路复用（Time Division Multiplex and Multiplexer，TDM）接口的密度。需要注意的是，只有 EVM 模块可在 EVM 插槽中使用。网络模块和 NME 不能用于此插槽，否则，可能将损坏该模块或路由器。此外，NME 插槽中不支持 EVM 模块。图 10-13 所示为 EVM 模块。

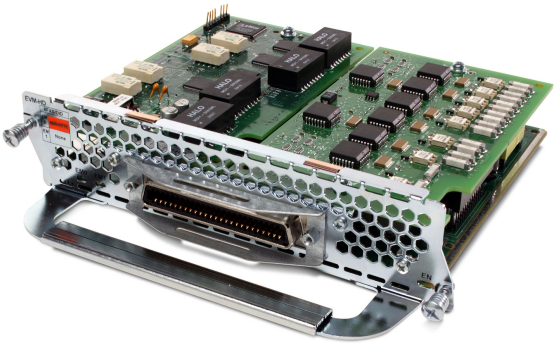


图 10-13　EVM 模块

10.2 路由器接口

通常情况下，路由器提供的局域网接口是非常丰富的，用户也可以根据本地网络类型选择相应接口类型的产品，例如以太网路由器。以太网中的网络接口类型通常包括双绞线接口、光纤接口两种。局域网接口主要用于网络中的核心层交换机或管理终端，并且大多数路由器都提供模块插槽，用户可根据需要安装相应的模块。

局域网接入广域网的方式有多种，如 DDN 接入、ADSL 接入、光纤接入等，为了满足用户的这种需求，路由器通常需要配备多种广域网接口。

10.2.1 10Base-T/100Base-TX/1000Base-T 接口

RJ-45 以太网接口是最为常见、且使用最多的接口类型，主要用于为路由器与局域网的连接提供廉价接口。如果必须通过光纤才能连接至远程网络或 ISP（Internet Service Provider，因特网服务提供商），则需要借助于收发转发器才能实现彼此之间的连接。根据接口的速率不同，可以将接口分为 10Base-T、100Base-TX 和 1000Base-T 三类。每种接口的标识各不相同，其中，10Base-T 接口通常标识为“ETHERNET”（如图 10-14 所示）。

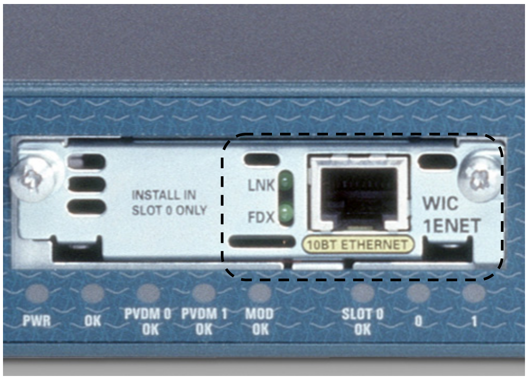


图 10-14 10Base-T 接口

100Base-TX 接口通常标识为“Fast Ethernet”或“FE”（如图 10-15 所示）。

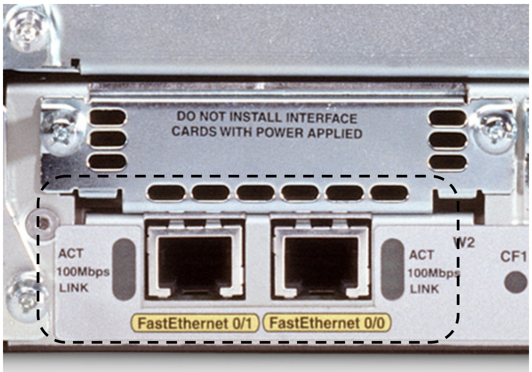


图 10-15 10/100Base-TX 接口

1000Base-T 接口通常标识为“GE”（如图 10-16 所示）。

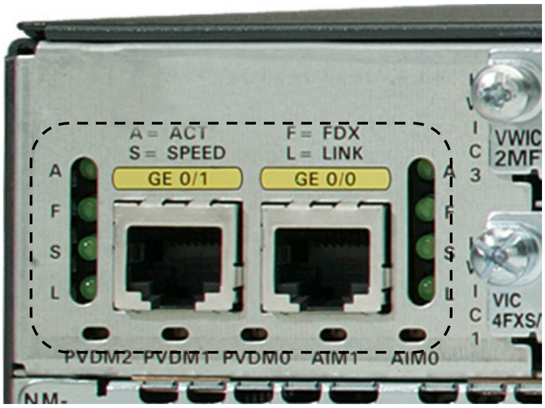


图 10-16　1000Base-T 接口

10.2.2 GBIC/SFP 插槽

路由器模块往往会提供 GBIC 或 SFP 插槽，用于适应不同的传输介质，借助相应的 GBIC/SFP 模块，可以实现千兆位网络连接。图 10-17 所示为 GBIC 插槽。

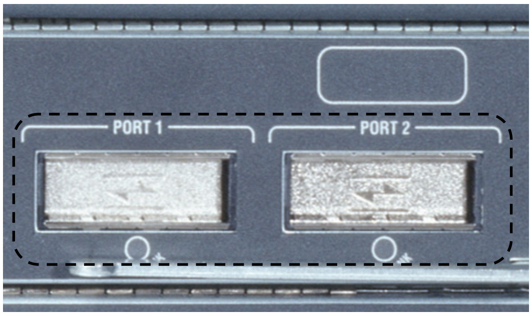


图 10-17　GBIC 插槽

图 10-18 所示为 SFP 插槽。SFP 是一种新型接口，被广泛应用于各类新款路由器模块。

图 10-18　SFP 插槽

10.2.3 SC/LC 接口

路由器的光纤接口类型主要有两种，即 SC 接口和 LC 接口。其中，SC 接口除了用于实现传统的快速以太网和千兆位以太网连接外，还被广泛应用于 FDDI 和 ATM 链路。如图 10-19 所示为 SC 光纤接口。

图 10-20 所示为 LC 光纤接口。与 SFP 插槽一样，LC 也是新型光纤接口，被广泛应用于各类新款路由器模块。

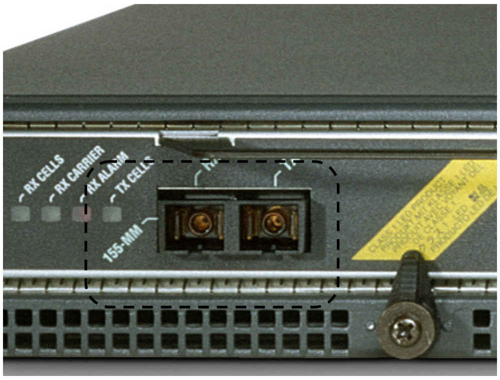


图 10-19　SC 光纤接口

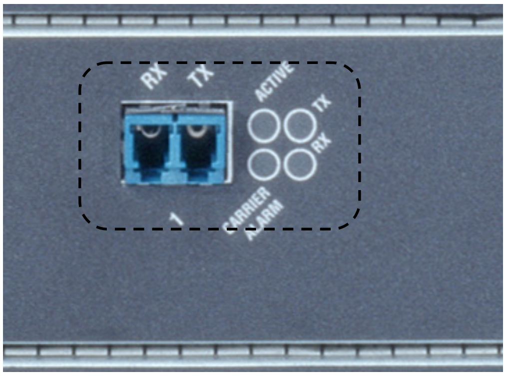


图 10-20　LC 光纤接口

10.2.4 T1/E1 接口

T1/E1 用于实现远程网络连接，传输介质可以是同轴电缆、双绞线或光纤。T1/E1 表示该连接具有高质量的通话和数据传送界面。其中，T1 是美国标准，为 1.544 Mbps；E1 是欧洲标准，为 2.048 Mbps。我国专线标准一般执行欧洲标准 E1，并根据用户的需要再进行信道分配（以 64 K 为单位）。例如，PPP 的 DDN 线路及帧中继线路等都可以使用 E1 线路。E1/T1 接口通常标识为“T1/E1”或“CTLR T1/E1”，如图 10-21 所示。

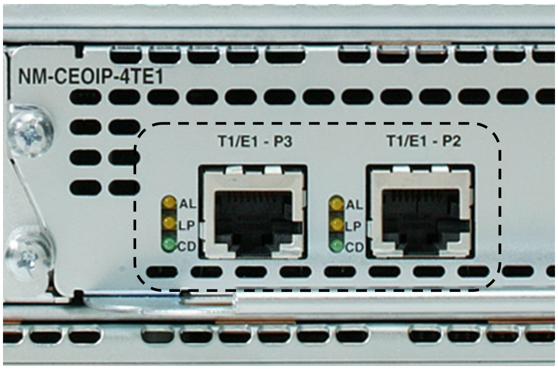


图 10-21　T1/E1 接口

一条 T1/E1 可以同时有多个并发信道，每个信道都是一个独立的连接。

T1 提供 23 个 B 信道和一个 D 信道，即 23B+D.1.544 Mbps。

E1 提供 30 个 B 信道和一个 D 信道，即 30B+D.2.048 Mbps。

E1 接口有两种配置情况：

- 作为信道化（Channelized）E1 接口使用。接口在物理上分为 31 个时隙，可以任意地将全部时隙分成若干组，每组时隙捆绑以后作为一个接口使用，其逻辑特性与同步串口相同，支持 PPP、帧中继、LAPB 和 X.25 等链路层协议。
- 作为非信道化（Unchannelized）E1 接口使用。接口在物理上作为一个 2 Mbps 速率的 G.703 同步串口，支持 PPP、帧中继、LAPB 和 X.25 等链路层协议。

知·识

时隙（Timeslot）专用于某一个单个通道的时隙信息的串行自复用的一个部分。在 T1 和 E1 服务中，一个时隙通常是指一个 64 Mbps 的通道。

10.2.5 智能串行接口

为在更小的空间内支持更高的端口密度，Cisco 开发了智能串行（Smart Serial）接口。智能串行接口可借助 HDLC（Cisco High-Level Data Link Control，高速数据链路控制）、PPP（Point-to-Point Protocol，点对点协议）或帧中继（Frame Relay），或更早的 SDLC（Synchronous Data Link Control，同步数据链路控制）和 X.25 等链路，为局域网提供串行广域网连接。智能串行接口可以兼容异步/同步（Asynchronous/Synchronous，A/S）串行接口，能够借助不同的电缆为路由器提供 EIA/TIA-232、EIA/TIA-449、V.35、X.21、DTE/DCE、EIA-530 或 EIA-530A 串行接口，实现与远程路由器的连接。

图 10-22 所示为 4 端口串行 HWIC 卡（HWIC-4T），拥有 4 个高速串行接口，同时支持异步和同步连接。

图 10-23 所示为 2 端口串行 HWIC 卡（HWIC-2SER），拥有 2 个高速串行接口，只支持同步连接。

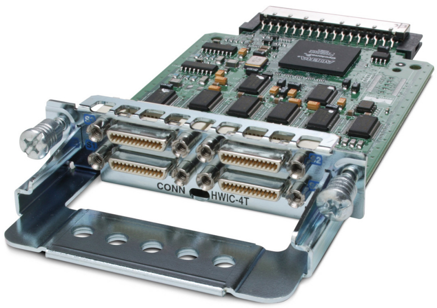


图 10-22　HWIC-4T

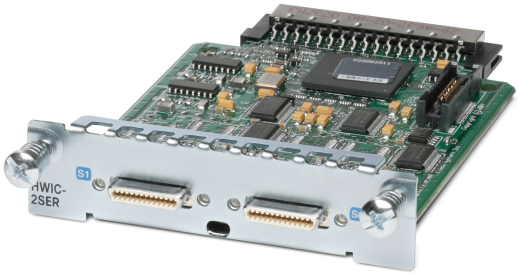


图 10-23　HWIC-2SER

10.2.6 异步/同步串口

异步串口（ASYNC）通常使用专用电缆连接至 MODEM 或 MODEM 池，用于实现远程计算机通过公用电话网拨入网络。

同步串口（SYNC）是典型的广域网端口，在广域网连接中应用比较广泛，如连接 DDN、帧中继（Frame Relay）、X.25、PSTN（模拟电话线路）等网络连接模式。在企业网之间有时也通过 DDN 或 X.25 等广域网技术进行专线连接。同步串口一般要求传输速率比较高，通过这种端口所连接的网络两端都要求实时同步。

异步/同步串口主要有两种类型，即 DB-60 和 EIA-232（也称为 RS-232）。图 10-24 所示为 DB-60 异步/同步串口。

图 10-25 所示为 8 端口异步/同步 HWIC 卡（HWIC-8A/S），拥有 8 个低速异步/同步 EIA-232 接口。

图 10-24　DB-60 异步/同步串口

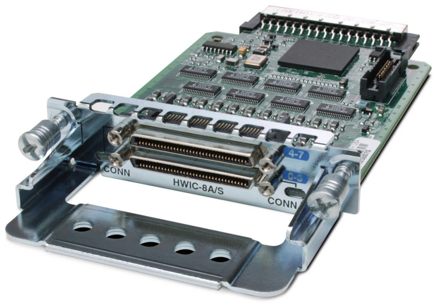


图 10-25　HWIC-8A/S

10.2.7 ADSL 接口

ADSL 接口用于连接 ADSL 链路，实现与远程路由设备的宽带连接。ADSL 接口往往被应用于中低端路由器，通常标识为“ADSL”，如图 10-26 所示。

图 10-26　ADSL 接口

10.2.8 BNC 接口

ATM 的传输介质常常是光纤，但是 100 m 以内的同轴电缆或 5 类双绞线也是可以的。图 10-27 所示为 BNC 接口的 T3/E3 模块，用于以同轴电缆作为传输介质的 ATM 网络。

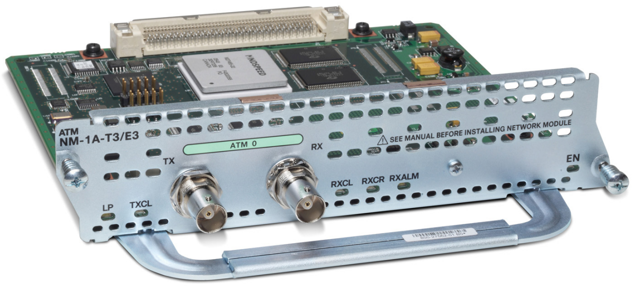


图 10-27　BNC 接口

10.3　路由器的连接

应用路由器的主要目的就是优化网络配置，为网络选择最佳通信路径。因此，为了保证资源的合理利用，以及实现高效快速地访问网络，无论是在局域网连接中还是在 Internet 接入中应用路由器，都应当按照最佳连接方式进行连接。

10.3.1　路由器连接策略

由于较大的数据传输都是在局域网内部进行的，所以，作为与 Internet 或其他网络进行互连的设备，路由器端口的传输速率大都不太高。一般情况下路由器的连接应当遵循以下策略。

- 由于路由器只在与 Internet 连接或与其他网络连接时才被用到，所以，应该将路由器放置于最频繁访问外网的位置。
- 在保障某些特别设备（如 Web 服务器）特殊需要的同时，要求网络内所有的计算机都享有同等访问路由器的机会。
- 如果没有特殊要求，路由器应当直接连接在核心层交换机上（如图 10-28 所示）。

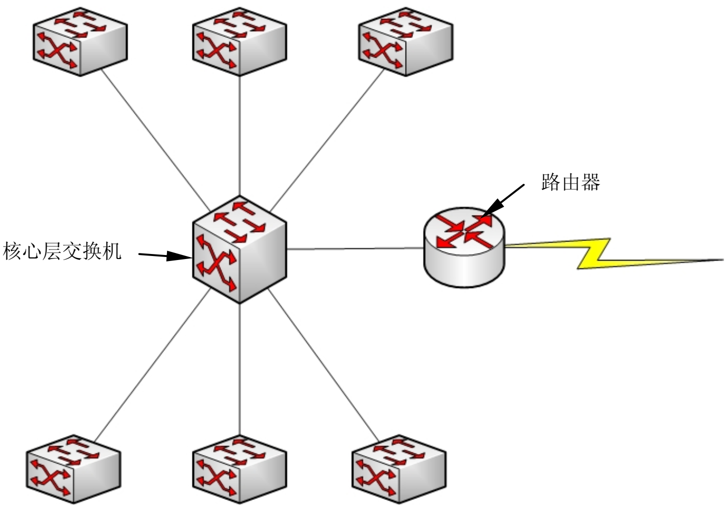


图 10-28　路由器连接在核心层交换机上

10.3.2 与局域网设备的连接

以光纤为传输介质连接路由器与交换机时，其光纤跳线的使用与连接方式和交换机之间的连接完全相同，此处不复赘述。

如果路由器和交换机均提供 RJ-45 端口，那么，可以使用双绞线跳线将交换机和路由器的两个端口连接在一起。需要注意的是，路由器和集线设备之间的连接不使用交叉线，而是使用直通线，也就是说，跳线两端的线序完全相同。

另外，路由器和交换机端口的传输速率应当尽量匹配，否则，应使交换机和路由器的端口速率均设置为自适应，以保证其连接速率和双工模式的一致。另外，应当尽量将路由器直接连接至汇聚层交换机，如图 10-29 所示。

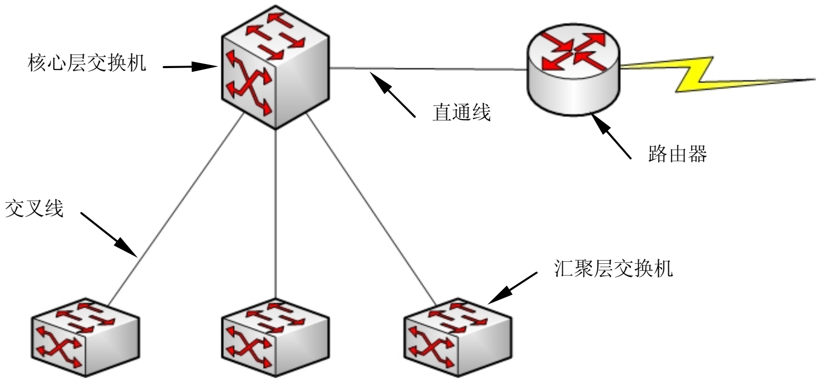


图 10-29　路由器与交换机之间的连接

10.3.3 连接器与电缆

1. 连接器

若欲连接不同类型的接口，必须使用与之适应的连接器。Cisco 路由器支持多种类型的接口，并提供了类型丰富的连接器，如 EIA/TIA-232 连接器（如图 10-30 所示）、EIA/TIA-449 连接器（如图 10-31 所示）、V.35 连接器（如图 10-32 所示）、X.21 连接器（如图 10-33 所示）和 EIA-530 连接器（如图 10-34 所示）。其中，上方为 DTE（数据终端设备，Data Terminal Equipment）连接器，下方为 DCE（数据通信设备，Data Communications Equipment）连接器。

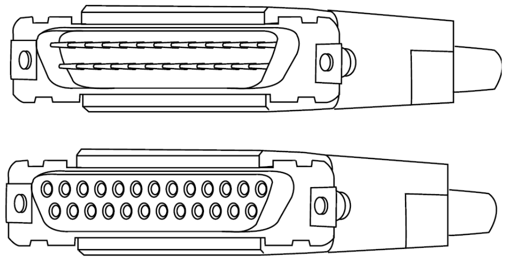


图 10-30　EIA/TIA-232 连接器

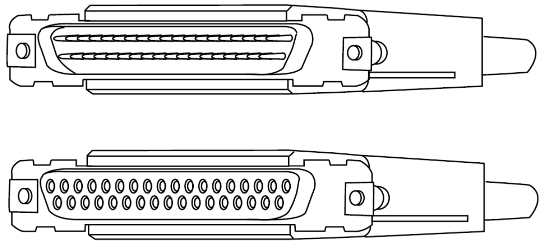


图 10-31　EIA/TIA-449 连接器

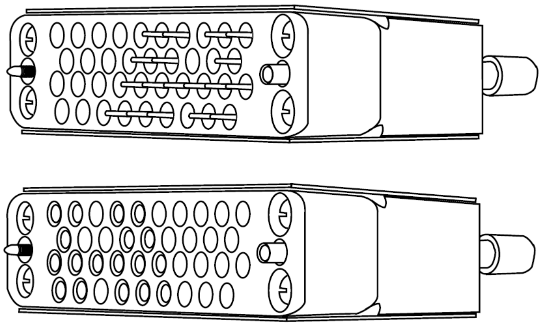


图 10-32　V.35 连接器

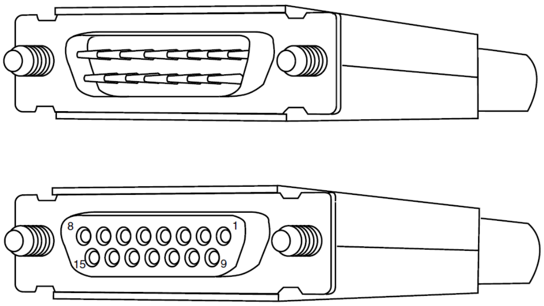


图 10-33　X.21 连接器

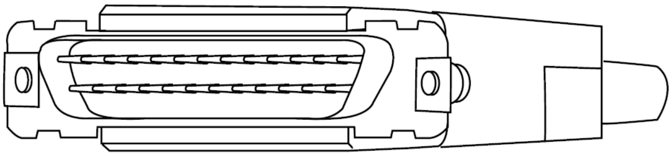


图 10-34　EIA-530 连接器

此外，还包括 BNC 连接器（如图 10-35 所示）、DB-26 连接器、DB-60 连接器和 RJ-48 连接器等。

图 10-35　BNC 连接器

2. 路由器电缆

所谓路由器电缆，就是适用于路由器之间、路由器与广域网设备之间连接的电缆。电缆的两端可以根据需要选择相同或不同的连接器。如图 10-36 所示，串行电缆的一端为 DB-60 连接器，另一端则依次分别为 EIA/TIA-232、EIA/TIA-449、V.35、X.21 和 EIA-350 连接器，用于连接不同类型的接口。

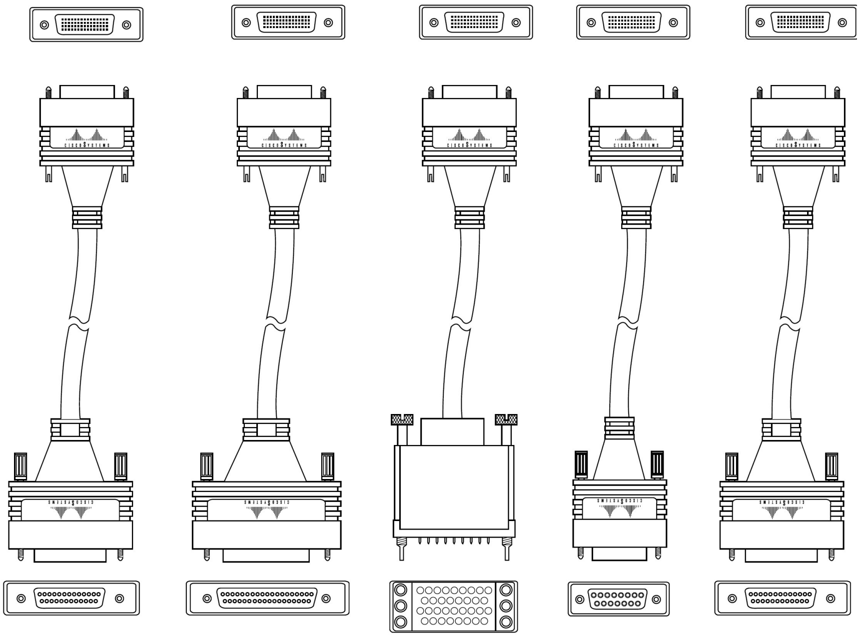


图 10-36　串行接口电缆

如图 10-37 所示，智能串行电缆的一端为 DB-26 连接器，另一端则依次分别为 EIA/TIA-232、EIA/TIA-449、V.35、X.21 和 EIA-350 连接器，用于连接不同类型的接口。

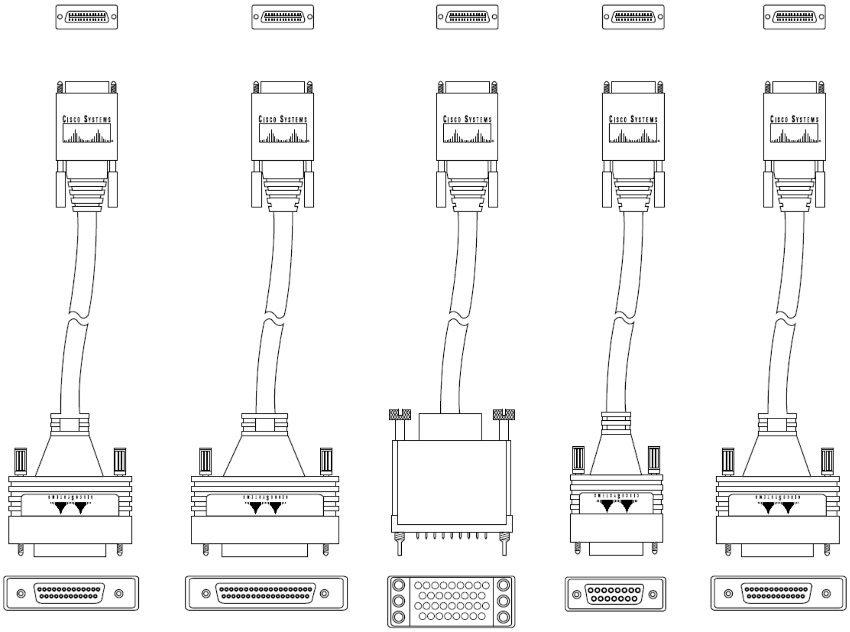


图 10-37　智能串行接口电缆

图 10-38 所示为 DB-60-EIA-232 串行电缆，图 10-39 所示为 DB-26-V.35 电缆。

图 10-38　DB-60-EIA-232 串行电缆

图 10-39　DB-26-V.35 电缆

10.3.4　与广域网接入设备的连接

1. 异步串行口连接

异步串行口主要提供与 Modem 的连接，用于实现远程计算机通过公用电话网拨入局域网络。除此之外，也可用于连接其他终端。当路由器通过线缆与 Modem 连接时，必须使用 RJ-45-to-DB-25 或 RJ-45-to-DB-9 适配器。路由器与 Modem 或终端之间的连接如图 10-40 所示。

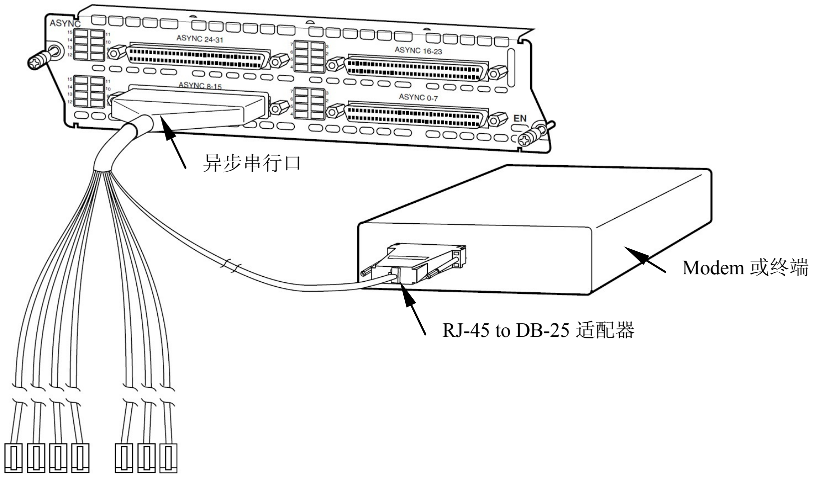


图 10-40　异步接口连接至异步设备

2. 同步串行口连接

根据广域网和 Internet 接入设备的不同，可分别采用不同的电缆将路由器的同步串行口与 Internet 设备连接在一起。图 10-41 所示为同步串行接口连接至 CSU/DSU（Channel Service Unit/Data Service Unit，信道服务单元/数据服务单元）。

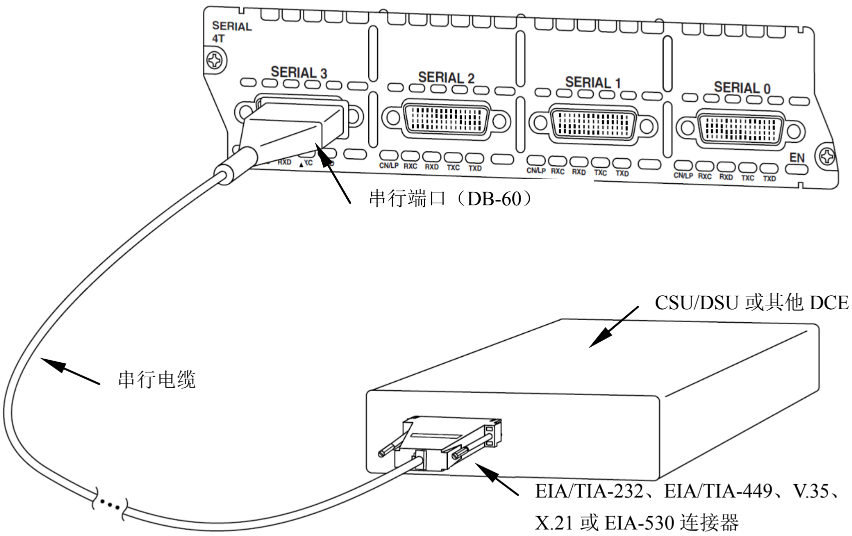


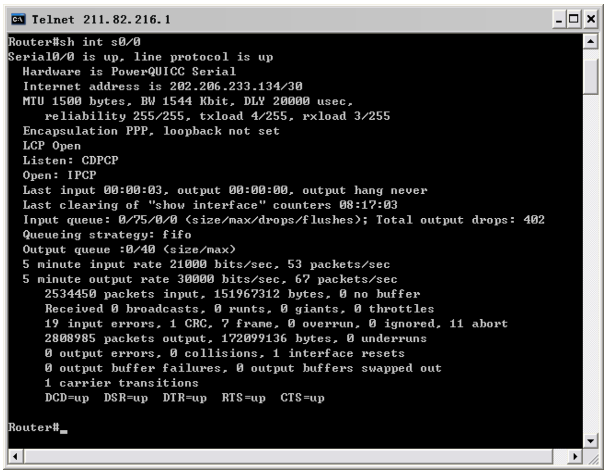
图 10-41　同步串行接口连接至 CSU/DSU

10.4　路由器的连接测试

当路由器相应的连接完成以后，必须进行测试，以判断路由器是否连接完好，各接口是否正常工作等，确保路由器正常工作。与交换机一样，路由器也可以通过 Show 命令和 LED 指示灯来进行测试。

10.4.1　Show 命令判断

使用 Show interface interface_id 命令也同样可以判断路由器各接口的工作状态。图 10-42 所示为串行接口正常工作状态，并有数据输入和输出。其他接口工作状态的判断与之类似，这里不再赘述。



```
Telnet 211.82.216.1
Router#sh int s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 202.206.233.134/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 4/255, rxload 3/255
  Encapsulation PPP, loopback not set
  LCP Open
  Listen: CDPCP
  Open: IPCP
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters 08:17:03
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 402
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 21000 bits/sec, 53 packets/sec
  5 minute output rate 30000 bits/sec, 67 packets/sec
     2534450 packets input, 151967312 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     19 input errors, 1 CRC, 7 frame, 0 overrun, 0 ignored, 11 abort
     2808985 packets output, 172099136 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Router#_
```

图 10-42　串行接口正常工作状态

10.4.2 LED 指示灯判断

借助路由器的 LED 指示灯，可以直观而快速判断系统工作状态和端口工作状态，从而有利于网络故障，特别是网络链路故障的诊断和排除。

1. Cisco 3825 路由器 LED 指示灯

路由器各接口的工作状态，也可以借由 LED 指示灯进行判断。图 10-43 所示为 Cisco 3825 路由器前面板 LED 指示灯，图 10-44 所示为 Cisco 3825 路由器后面板 LED 指示灯。

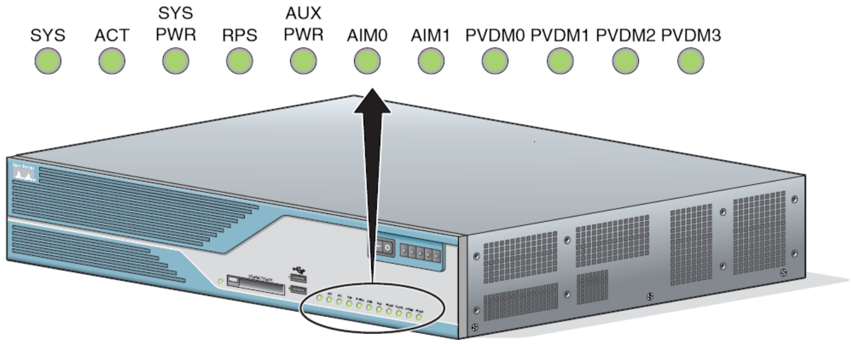


图 10-43　Cisco 3825 路由器前面板 LED 指示灯

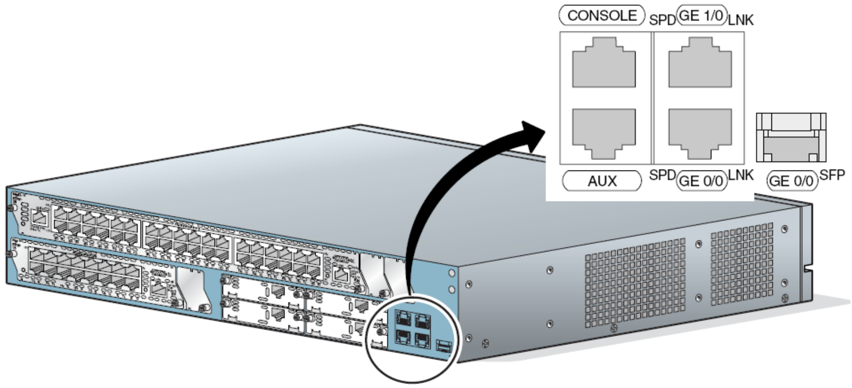


图 10-44　Cisco 3825 路由器后面板 LED 指示灯

2. Cisco 3845 路由器 LED 指示灯

图 10-45 所示为 Cisco 3845 路由器前面板 LED 指示灯，图 10-46 所示为 Cisco 3845 路由器后面板 LED 指示灯。

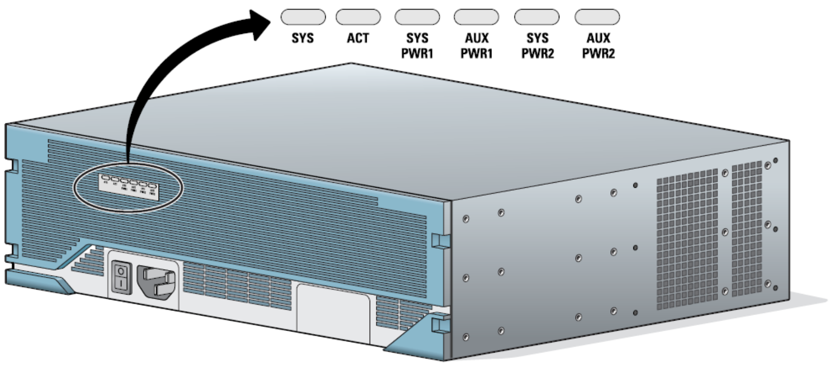


图 10-45　Cisco 3845 路由器前面板 LED 指示灯

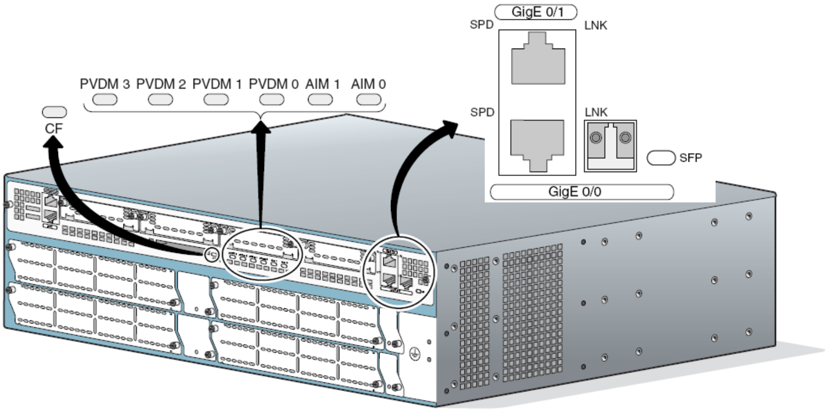


图 10-46　Cisco 3845 路由器后面板 LED 指示灯

下面，以 Cisco 2800/3800 系列路由器为例，介绍一下 LED 指示灯的颜色、状态及其含义，如表 10-1 所示。

表 10-1　Cisco 2800/3800 路由器 LED 指示灯的颜色、状态及其含义

LED	颜色和状态	含　义
SYS	关	路由器电源未接通
	稳定的绿色	正常运行
	闪烁绿色	引导或处于 ROM 监控模式下
	琥珀色	已加电但出现故障
ACT	关	无信息包活动
	稳定显示绿色或闪烁绿色	信息包活动
SYS PWR	关	路由器的电源未接通
	稳定的绿色	正常运行
RPS	关	连接到主电源系统
	稳定的绿色	连接到冗余电源系统
SYS PWR1	关	电源系统 1 不存在
	稳定的绿色	存在并启用
	琥珀色	存在但出现故障
SYS PWR2	关	电源系统 2 不存在
	稳定的绿色	存在并启用
	琥珀色	存在但出现故障

（续表）

LED	颜色和状态	含　义
AUX PWR	关	IP 电话电源断开
	稳定的绿色	正常运行
	琥珀色	已加电但出现故障
AUX PWR1	关	IP 电话电源系统 1 不存在
	稳定的绿色	存在并启用
	琥珀色	已加电但出现故障
AUX PWR2	关	IP 电话电源系统 2 不存在
	稳定的绿色	存在并启用
	琥珀色	已加电但出现故障
AIM0	关	AIM0 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
AIM1	关	AIM1 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
PVDM0	关	PVDM0 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
PVDM1	关	PVDM1 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
PVDM2	关	PVDM2 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
PVDM3	关	PVDM3 不存在
	绿色	存在并启用
	琥珀色	存在但出现故障
CF	关	未访问紧凑式闪存
	稳定的绿色	正在访问紧凑式闪存；不能将紧凑式闪存卡拔出
	闪烁绿色	正在访问紧凑式闪存；不能将紧凑式闪存卡拔出
SFP	关	未建立 SFP 链接
	绿色	SFP 端口激活，已建立链接
GE0:链接	关	没有链接
	绿色	存在以太网电缆，已建立链接
GE0:速度	闪烁绿色	闪烁频率指示端口速度
GE1:链接	关	没有链接
	绿色	存在以太网电缆，已建立链接
GE1:速度	闪烁绿色	闪烁频率指示端口速度
PS1	关	未提供备用电源
	闪烁绿色	提供并使用备用电源
	琥珀色	虽提供但已关闭，或者故障
PS2	关	未提供备用电源
	闪烁绿色	提供并使用备用电源
	琥珀色	虽提供但已关闭，或者故障

第 11 章　路由器的配置方式与初始化

路由器的配置方式与交换机基本相同。除了都可以采用图形化界面配置以外，也都支持使用 CLI 命令行进行配置。由于交换机与路由器的许多 CLI 配置命令完全相同，因此，两者之间的配置差异并不大。

11.1　路由器配置前的规划

对于局域网而言，路由器往往就是指边缘路由器，即用于实现与其他网络或 Internet 连接所使用的路由器。因此，路由器通常都位于网络中心。当然，在配置路由器之前，一定要与交换机、客户端统筹规划 IP 地址、主机名称、安全策略等。

1.　IP 地址规划

IP 地址的规划包括以下几个方面的内容。

- 内网 IP 地址规划。内网的 IP 地址规划，除了为不同 VALN 分配 IP 地址之外，还要为路由器的局域网端口划分 VLAN，指定 IP 地址段，并为路由器的局域网接口指定内网的 IP 地址。
- 外网 IP 地址规划。合理分配由 ISP 提供的合法 IP 地址。当然，路由器的 WAN 口至少需要一个合法 IP 地址。如果分配有更多的合法 IP 地址，应当考虑给放置于外网的服务器分配合法的 IP 地址。
- 内部服务器 IP 地址规划。如果服务器置于局域网内部，那么，一般应当为服务器单独指定一个 VLAN，然后，再在路由器上做 NAT 端口地址映射，实现内部服务器的 Internet 发布。
- VPN 内网 IP 地址规划。如果在路由器上配置 VPN 服务，那么，也应当为 VPN 客户端规划内网 IP 地址，以便其安全访问内部网络。

2.　名称规划

名称规划包括以下几个方面的内容。

- 每个接口所连接设备的名称，用于确认该接口所连接的网络或设备，便于日后实现对该接口的远程管理。接口注释中建议包含接口所连接的网络信息、设备信息等，便于日后对接口的管理。
- 每台路由器的名称。如果网络内拥有多台路由器，那么，应当为每台路由器分别命名，用于确认该路由器所处的位置，便于与其他路由器区分，并对该路由器实现远程管理。路由器名称中建议包含路由器的型号信息、位置信息或用途信息，便于对路由器的识别与管理。

3. 安全规划

安全规划包括以下几个方面的内容。

- 安全访问列表。确定在路由器上使用哪些访问列表，用于禁止在某个时间段访问网络、禁止访问某些 TCP 或 UDP 端口、禁止使用某些 IP 协议、限制某些 IP 地址范围内计算机的网络访问权限等。
- NAT 地址转换。是否采用 NAT 地址转换的方式实现 Internet 连接共享，并实现对内部网络计算机的保护。
- IOS 防火墙。是否启用 IOS 防火墙，以及启用哪些安全特性，如通信过滤、基于策略的多端口支持、网络地址转换、事件日志记录、虚拟专用网络、基于上下文的访问控制、JAVA 阻断、服务拒绝检测/预防、审计踪迹、实时告警等。

4. 接口规划

接口规划包括以下几个方面的内容。

- 接口连接。哪个接口连接到局域网，哪个接口连接到广域网（或 Internet），哪个接口用于备份线路。
- 接口类型和速率。每个接口采用哪种传输介质、哪种接口类型。

11.2 路由器配置源与配置方式

路由器的配置与交换机的配置非常相似，一般都是先借助计算机和控制台端口进行初始化，然后，再借助 CLI 命令行或其他网络管理工具进行管理。另外，由于路由器用于实现不同网络之间的通信，因此，在没有完成配置之前，路由器所有端口都将处于 shutdown 状态，当然，网络之间也是无法连通的。

11.2.1 路由器的外部配置源

通常情况下，可以通过 3 种手段配置用于计算机与路由器之间的连接，即通过 Console 端口直接连接的方式、通过网络设备间接连接的方式、通过 AUX 端口远程连接的方式。

由于路由器没有自己的键入设备所以在对路由器进行配置时，一般都是通过另一台计算机连接到路由器的各种接口上进行配置，这些配置的方法称为外部配置源，如图 11-1 所示。

- 控制台

将计算机的串口（COM 口）通过 Console 线与路由器的 Console 端口相连；或者，将计算机的 USB 接口通过 USB 线缆与路由器的 mini-USB Console 端口连接，并在计算机上运行终端仿真软件（如超级终端），与路由器进行通信，完成路由器的配置。

- AUX

AUX 串行口可以连接调制解调器，网络管理员以电话拨号方式，对路由器进行远程配置和管理。

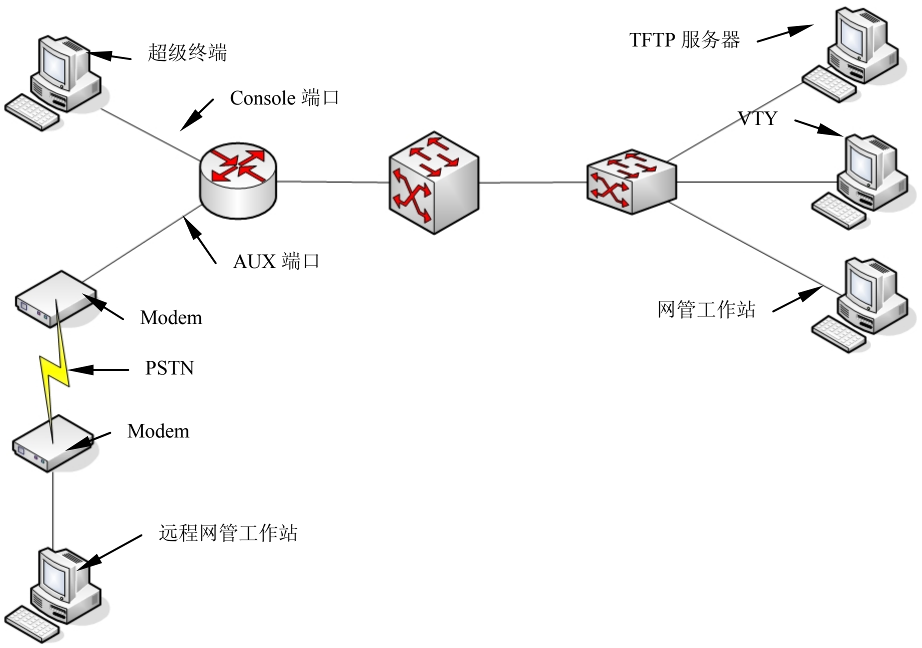


图 11-1　外部配置源

- 虚拟终端（Telnet）

如果路由器已有一些基本配置，至少配置了局域网接口或广域网接口的 IP 地址，就可通过运行 Telnet 程序的计算机作为路由器的虚拟终端与路由器建立通信，完成对路由器的配置与管理。

- 网管工作站

路由器可通过运行网络管理软件的网管工作站进行配置，如 Cisco SDM、CiscoWorks、HP OpenView 等。

- TFTP 服务器

TFTP（Trivial File Transfer Protocol）是一个 TCP/IP 简单文件传输协议，可将配置文件从路由器传送到 TFTP 服务器上，也可将配置文件从 TFTP 服务器传送到路由器上。TFTP 不需要用户名和口令，使用非常简单。

11.2.2 路由器的配置接口

与交换机一样，路由器也没有自己的输入设备，所以，配置时都是通过专用电缆将计算机与路由器的配置接口进行连接，在计算机上完成相关配置操作。路由器的配置接口有两个：Console 接口和 AUX 接口。Console 接口通常用来进行路由器的基本配置，通过专用 Console 线连接到计算机，而 AUX 接口则用于路由器的远程配置连接。

1. Console 接口

Console 接口是典型的配置接口。使用 Console 线直接连接至计算机的串口，利用终端仿真程序（一般使用 Windows 自带的“超级终端”）在本地配置路由器。路由器的 Console 接口

多为 RJ-45 接口，并标记有“CONSOLE”字样。图 11-2 所示为 Console 接口。

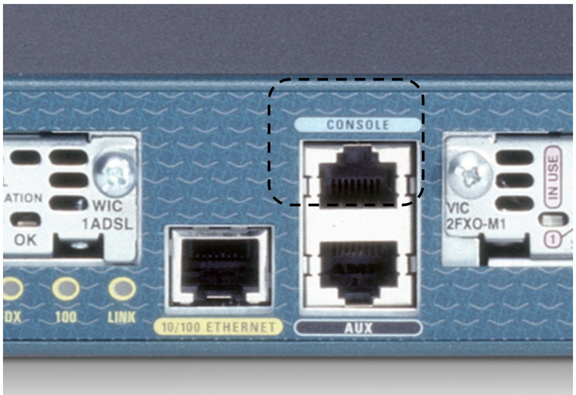


图 11-2　Console 接口

Cisco 2900/3900 系列路由器同时提供了 mini-USB 接口作为 Console 接口（如图 11-3 所示），只需使用普通的 USB 电缆，即可实现对路由器的配置与管理。

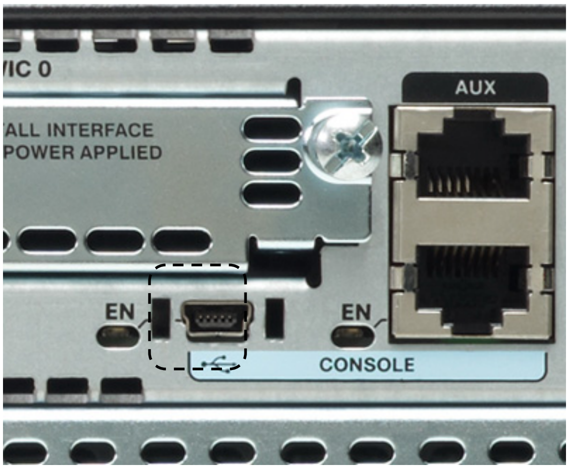


图 11-3　mini-USB 接口

2. AUX 接口

AUX 接口为异步接口，主要用于远程配置，也可用于拨号备份，可与 MODEM 连接。支持硬件流控制（Hardware Flow Control）。AUX 接口与 Console 接口通常被放置在一起，并标记有“AUX”字样。

11.2.3 路由器与配置终端设备的连接

配置路由器除了可以借助 Console 口外，还可以借助 AUX 口进行远程配置。路由器与配置终端之间的连接，非常类似于交换机与配置终端之间的连接，既可以使用普通的 USB 电缆（如图 11-4 所示），也可以使用传统的 Console 线。

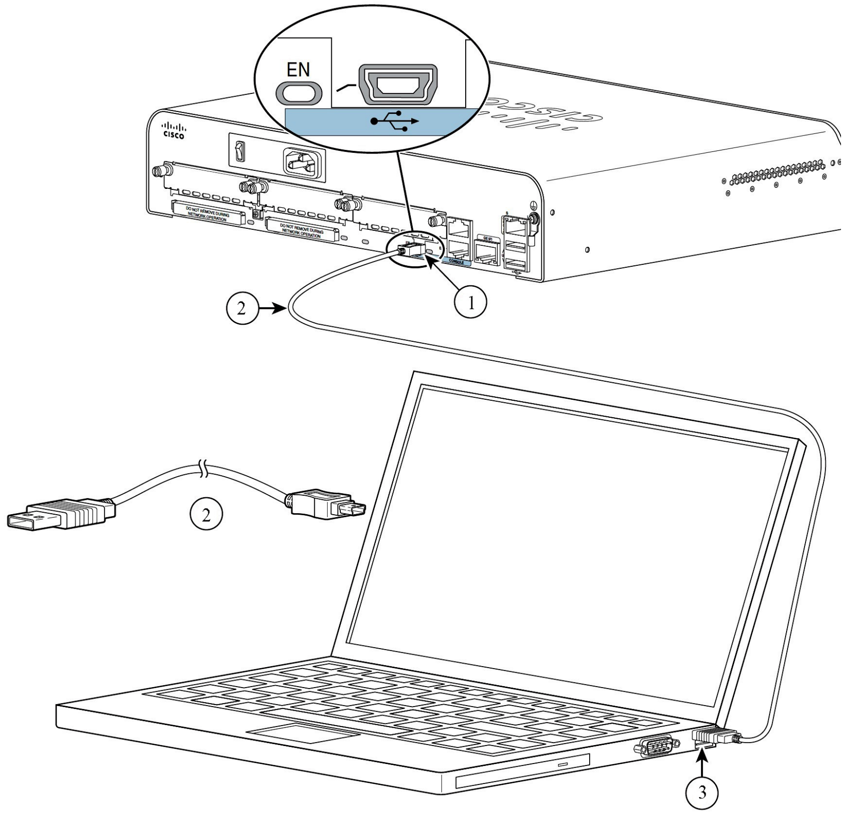


图 11-4 借助 Console 端口配置路由器

注：① 路由器 Mini-USB 接口 ② USB 电缆 ③ 计算机 USB 接口

另外，路由器与可以借助传统的电话线和 Modem，以 AUX 端口从远程实现对路由器的配置和管理。借助 AUX 端口进行远程管理时，路由器与 Modem 之间的连接如图 11-5 所示。

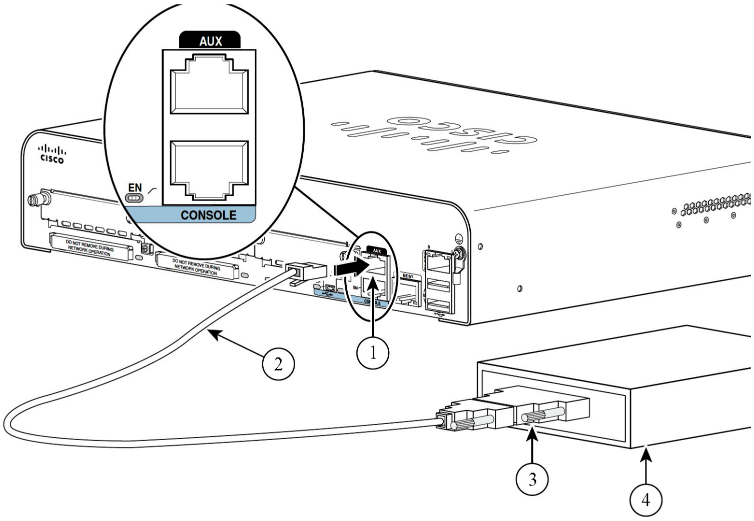


图 11-5 借助 AUX 端口配置路由器

注：① 路由器 AUX 接口 ② Console 电缆 ③ 适配器 ④Modem

11.2.4 路由器的配置方式

可以采用各种灵活多样的方式实现对路由器的配置与管理。通常情况下，可以借助超级终端、Telnet 和 Cisco CP 完成所有工作任务。

借助超级终端和 Telnet 管理路由器时，其配置和管理方式与交换机非常相似，此处不复赘述，请参见“第 5 章交换机配置方式与初始化”中的相关内容。需要注意的是，路由器的 CLI 命令模式与交换机的 CLI 命令模式稍有差别。如表 11-1 所示为路由器的 CLI 命令模式。

表 11-1 路由器的 CLI 命令模式

	访问方法	提 示 符	退出方法	用 途
User EXEC（用户模式）	登录	Router>	使用 logout 或 exit 命令	● 改变终端配置 ● 平台基本测试 ● 显示设备状态
Privileged EXEC（特权模式）	在用户模式下，使用 enable 命令进入	Router#	使用disable或exit命令返回至用户模式	● 使用 show 和 debug 命令 ● 将系统映像拷贝至设备 ● 重新启动设备 ● 管理设备配置文件 ● 管理设备文件系统
Global configuration（全局配置模式）	在特权模式下，使用 configure terminal 命令进入	Router(config)#	使用 exit 或 end 命令返回至特权模式	配置设备
Interface configuration（接口配置模式）	在全局模式下，使用 interface 命令进入	Router(config-if)#	使用 exit 命令返回至全局模式，或使用 end 命令返回至特权模式	配置指定的接口
Line configuration（线路配置模式）	在全局模式下，使用 line vty 或 line console 命令进入	Router(config-line)#	使用 exit 命令返回至全局模式，或使用 end 命令返回至特权模式	配置指定的终端线路
ROM monitor（ROM 监控模式）	在特权模式下，使用 reload 命令，在系统引导的前 60 s 内一直按住 Break 键	rommon # >	使用 continue 命令	● 当有效映像不能装载时，以默认运行模式运行 ● 当系统缺乏有效映像而无法引导时，访问 fall-back 程序以装载映像 ● 在系统加电或重新装载 60 s 内，按下 Ctrl-Break 组合键进行密码恢复

路由器 CLI 各种命令模式的进入流程如图 11-6 所示。

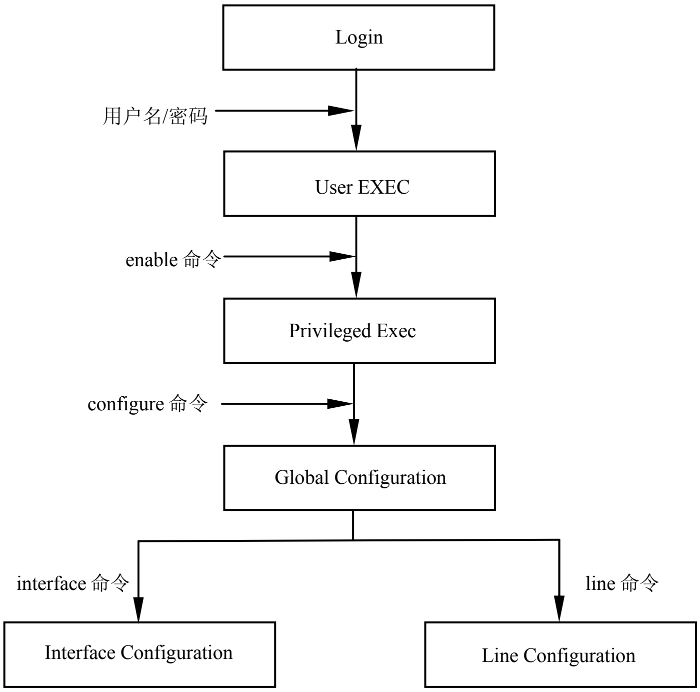


图 11-6　命令模式的进入流程

CLI 各种命令模式的退出流程如图 11-7 所示。

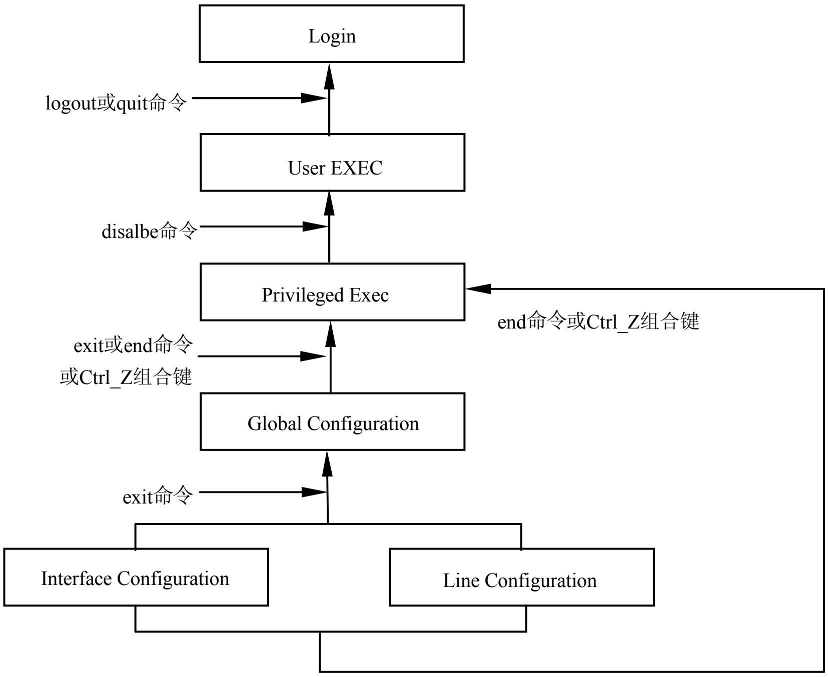


图 11-7　命令模式的退出流程图

Cisco CP（Cisco Configuration Professional）是 Cisco 专门为中低端路由器开发的图形化管理软件，特别适用于没有经过专业训练的网络管理员。Cisco CP 既可直接用于实现路由器的初始化，也可在路由器初始化完成之后，实现对路由器的图形化配置、管理、监控和故障诊断等任务。Cisco CP 作为 Cisco SDM 的替代产品，被广泛应用于中低端新型路由器产品，如 Cisco 800 系列、Cisco 1800/2800/3800 系列和 Cisco 1900/2900/3900/4400 系列路由器。图 11-8 所示为 Cisco CP 主界面。

图 11-8　Cisco CP 主界面

11.3　路由器初始化配置

路由器的初始化可以采用 3 种不同的方式，即借助设置命令工具初始化、以手工方式初始化和借助 Cisco SDM 应用程序进行初始化。由于 Cisco SDM 初始化采用图形界面进行操作，因此，相对而言，借助 SDM 进行初始化相对简单。不过，当路由器中没有安装 Cisco SDM 时，则必须采用 CLI 命令行方式进行初始化。

11.3.1　使用设置命令工具初始化配置

当一个全新的路由器第一次打开电源时，或者想重新配置路由器时，都可以在路由器初始化向导的指引下，实现对路由器的快速配置，完成路由器的最基本配置，并为以后的远程配置和管理做好准备。使用设置命令工具，配置路由器的主机名，设置密码，以及如何配置接口，以便与管理网络通信。

设置命令工具提示输入与路由器和网络相关的基本信息，并创建初始配置文件。创建配置文件后，可使用 CLI 或 Cisco 路由器和安全设备管理器（SDM）执行其他配置。设置命令工具的具体提示内容视路由器型号、已安装的接口模块和软件映像的情况而定。下列示例和用

户项（以粗体显示）仅作为示例显示。

注·意　如果使用设置命令工具时出错，可以先退出，然后再次运行设置命令工具。按 Ctrl+C 组合键，然后在授权 Exec 模式提示符（Router#）下输入 setup 命令。

① 若欲使用安装命令工具，结束后输入 yes。

--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes/no]:

② 当下列信息出现时，按 Enter 键进入基本管理设置。

Continue with configuration dialog? [yes/no]:
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

③ 输入路由器的主机名（本示例使用 Router）。

Configuring global parameters:
Enter host name [Router]:**BYRouter**

④ 输入特权加密密码。该密码是加密的（更安全），并且查看配置时不能看到它。

The enable secret is a password used to protect access to
privileged Exec and configuration modes.This password, after
entered, becomes encrypted in the configuration.
Enter enable secret:**xxxxxx**

⑤ 输入不同于特权加密密码的特权密码。该密码未加密（不十分安全）并且查看配置时能看到它。

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password:**xxxxxx**

⑥ 输入虚拟终端密码，此密码防止通过控制台端口以外的端口进行未授权的访问。

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password:**xxxxxx**

⑦ 根据网络的具体情况对下列提示给出合适的响应。

Configure SNMP Network Management?[yes]:
Community string [public]:
显示可用接口的汇总。

注·意 显示的接口编号视 Cisco 模块化路由器平台的类型和已安装的接口模块及接口卡而定。

Current interface summary
Controller Timeslots D-Channel Configurable modes Status
T1 0/0/0 24 23 pri/channelized Administratively up
T1 0/0/1 24 23 pri/channelized Administratively up
T1 0/2/0 24 23 pri/channelized Administratively up
T1 0/2/1 24 23 pri/channelized Administratively up
Any interface listed with OK? value "NO" does not have a valid configuration
Interface IP-Address OK?Method Status Protocol
GigabitEthernet0/0 unassigned NO unset up up
GigabitEthernet0/1 unassigned NO unset up up

⑧ 选择一个可用接口，以将路由器连接到管理网络。

Enter interface name used to connect to the
management network from the above interface summary:gigabitethernet0/0

⑨ 根据网络的具体情况对下列提示给出合适的响应。

Configuring interface GigabitEthernet0/0:
Use the 1000Base-T（RJ-45） connector?[yes]:yes
Operate in full-duplex mode?[no]:no
Configure IP on this interface?[yes]:yes
IP address for this interface: 10.0.0.2
Subnet mask for this interface [255.0.0.0] : 255.255.255.248
Class B network is 10.0.0.2, 29 subnet bits; mask is /29

⑩ 显示配置。

```
The following configuration command script was created:
hostname BYRouter
enable secret 5 $1$D5P6$PYx41/lQIASK.HcSbfO5q1
enable password xxxxxx
line vty 0 4
password xxxxxx
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/0
no shutdown
```

media-type 1000Base-T
half-duplex
ip address 10.0.0.2 255.255.255.248
!
interface GigabitEthernet0/1
shutdown
no ip address
!
end

⑪ 对下列提示给出响应，选择 [2] 保存初始配置。

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!RETURN

出现用户提示：

Router>

⑫ 验证初始配置。

- 要验证接口运行是否正确，接口和线路协议是否处于正确状态（上或下），输入 show interfaces 命令。
- 要显示已为 IP 配置的接口的汇总状态，输入 show ip interface brief 命令。
- 要验证是否已配置正确的主机名和密码，输入 show configuration 命令。

完成并验证了初始配置后，Cisco 路由器准备好进行特定功能的配置。

> **注意** 在全局配置模式下，输入 setup 命令，也可以进入初始化配置工具，对路由器进行重新设置。

11.3.2 使用 CLI 命令手动初始配置

当然，也可以选择采用手工方式，以 CLI 命令初始配置路由器。主要的初始配置内容包括：

- 配置路由器主机名（可选）
- 配置 Enable 或 Enable Secret 密码（必须）
- 配置 Console 空闲超时（可选）
- 配置以太网、快速以太网、千兆位以太网端口（必须）
- 指定默认路由或网关

- 配置 IP 路由和 IP 协议（必须）
- 配置 VTY（必须）
- 配置 AUX（可选）
- 校验网络连接（必须）
- 保存路由器配置（必须）
- 备份配置和系统映像（可选）

--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog?[yes/no]:

> **提・示** 如果这些信息不出现，则出厂时已将 SDM 和默认配置文件安装到路由器上。

① 要继续使用 CLI 进行手动配置，在启动信息结束时输入 no。
Would you like to enter the initial configuration dialog?[yes/no]:no
② 按 Return 停止自动安装，继续进行手动配置。
Would you like to terminate autoinstall?[yes] Return
出现几条信息，以与下列相似的行结束：
...
Copyright (c) 1986-2012 by cisco Systems, Inc.
Compiled <date> <time> by <person>
③ 按回车键，显示 Router> 提示符。
...
flashfs[4]:Initialization complete.
Router>
④ 输入特权 Exec 模式。
Router> enable
Router#
⑤ 进入全局配置模式。
Router# configure terminal
Router(config)#
⑥ 配置路由器名称（本例为 BYRouter）。
Router(config)# hostname *BYRouter*
BYRouter(config)#
⑦ 配置 Enable 访问密码。
BYRouter(config)# enable password *password*
⑧ 选择局域网接口（本例为 gigabitethernet 0/0），进入接口配置模式。

BYRouter(config)# intface gigabitethernet 0/0

BYRouter(config-if)#

⑨ 为该接口配置 IP 地址信息（本例 IP 地址为 192.168.11.3，子网掩码为 255.255.255.248）。

BYRouter(config-if)# ipaddress 192.168.11.3 255.255.255.248

⑩ 激活该局域网接口。

BYRouter(config-if)# no shutdown

⑪ 返回全局配置模式。

BYRouter(config-if)# exit

BYRouter(config)#

⑫ 配置 Console 控制台，进入 Line 配置模式。

BYRouter(config)# line console 0

BYRouter(config-line)#

⑬ 设置特权 Exec 配置模式超时，指定在用户多长时间没有操作之后，将视为超时并自动退出配置模式（本示例超时设置为 2 分 30 秒，如果设置为 0 分 0 秒，则表示为不超时）。

BYRouter(config-line)# exec-timeout 2 30

⑭ 返回特权 Exec 配置模式。

BYRouter(config-line)# exit

BYRouter(config)#

⑮ 配置远程 Telnet 虚拟终端服务（Virtual Terminal Lines，VTY），指定最大允许访问的用户量（本例最多允许 5 位用户同时访问），进入 Line 配置模式。

BYRouter(config)# line vty 0 4

BYRouter(config-line)#

⑯ 配置 telnet 访问密码。

BYRouter(config-line)# password *password*

⑰ 在登录时启用密码检查。

BYRouter(config-line)# login

⑱ 返回特权 Exec 配置模式。

BYRouter(config-line)# end

BYRouter#

⑲ 查看并校验配置。

Router# show running-config

注意 为避免丢失已完成的工作，确保在执行过程中时常保存配置。使用 copy running-config startup-config 命令将配置保存到 NVRAM。

11.3.3 使用 Cisco CP Express 初始配置

如果路由器中已经安装了 Cisco CP（新型路由器默认安装该软件），那么，就可以使用

Cisco CP Express 以图形化界面的方式实现对路由器的初始化配置。Cisco CP Express 是 Cisco CP 的简化版本，可以完成对路由器的初始化配置和一些基本功能的快速配置。

1. Cisco CP 适用的路由器型号

Cisco Configuration Professional（Cisco CP）是用于 Cisco 接入路由器的 GUI 型设备管理工具。该工具通过简单易用的 GUI 向导，简化了路由、防火墙、IPS、VPN、统一通信、广域网和局域网配置，便于网络管理员更加轻松自由地部署路由器。Cisco CP 提供了一键式路由器锁定及创新的语音和安全审核功能，可用于检查路由器配置并提出更改建议，并可用于监控路由器状态，并对广域网和虚拟专用网（VPN）连接问题进行故障诊断。

Cisco CP Express 是 Cisco CP 的轻便版，可用于配置路由器局域网和广域网接口上的基本安全功能。Cisco CP Express 位于路由器闪存上。几乎所有新型 Cisco 路由器和 Cisco IOS Software 版本均可以支持 Cisco CP，例如 Cisco 800 系列、Cisco 1800 系列、Cisco 2800 系列、Cisco 3800 系列、Cisco 1900 系列、Cisco 2900 系列和 Cisco 3900 系列路由器都支持 Cisco CP（如表 11-2 所示）。

表 11-2　支持 Cisco CP 的路由器型号及 IOS 版本

路由器型号	支持 CCP 的最低 IOS 版本
Cisco 815	11.4(11)T
Cisco 850 系列	11.4(9)T
Cisco 861	11.4(20)T
Cisco 867	15.0(1)M
Cisco 870 系列	11.4(9)T
Cisco 881	11.4(20)T
Cisco 886	15.0(1)M
Cisco 887	15.0(1)M
Cisco 888	11.4(20)T
Cisco 890 系列	15.0(1)M
Cisco 1801 Cisco 1802 Cisco 1803	11.4(9)T
Cisco 1805	11.4(15)XY
Cisco 1811 Cisco 1812	11.4(9)T
Cisco 1841	11.4(9)T
Cisco 1861	11.4(20)T
Cisco 1941 Cisco 1941W	15.0(1)M
Cisco 2800 系列	11.4(9)T
Cisco 2900 系列	15.0(1)M
Cisco 3800 系列	11.4(9)T
Cisco 3900 系列	15.0(1)M

2. Cisco 路由器准备

Cisco CP Express 和 Cisco CP 需要进行以下基本配置才能连接到路由器并进行管理。

- 必须通过本地身份验证启用 http 或 https 服务器。
- 必须配置具有特权级别 15 和随附密码的本地用户账户。
- 必须通过本地身份验证启用使用协议 ssh/telnet 的 vty 线路。交互命令需要此配置。
- 必须配置 http 超时策略，以避免发生已知的 Cisco CP 启动问题。
- 必须将运行 Cisco CP 的计算机和启动 Cisco CP 的接口配置为使用相同子网的 IP 地址。

有两种方式可确保路由器配置满足上述要求。

- 将默认配置文件从路由器闪存复制到路由器 NVRAM。
- 使用 Cisco IOS CLI 输入所需的配置命令。

■ 将默认配置文件复制到路由器 NVRAM

出厂默认配置包括支持 Cisco CP 所需的所有命令，并使用 IP 地址 10.10.10.1 配置以太网接口。若欲恢复支持 Cisco CP 的默认配置启动，需将默认配置文件从路由器闪存复制到 NVRAM。操作如下：

① 通过控制台端口或以太网端口登录到路由器。

② 如果使用控制台端口，且路由器中没有正在运行的配置，将自动启动 Setup Command Facility，并显示以下文本。

```
--- System Configuration Dialog ---
Continue with configuration dialog?[yes/no]:
```

输入 no，然后可以直接输入 Cisco IOS CLI 命令。

如果 Setup Command Facility 没有自动启动，则表示有正在运行的配置，应转到下一步。

③ 路由器显示用户 Exec 模式提示符时，输入 enable 命令及其密码（如已配置）。

```
Router> enable
password password
Router#
```

④ 要标识默认配置文件，输入 show flash 命令。其文件名格式是 cpconfig-modelnumber.cfg，其中 modelnumbe 表示路由器系列号。例如，Cisco 860 和 880 系列路由器的配置文件名是 cpconfig-8xx.cfg。

```
Router# show flash
-#- --length-- -----date/time------ path
1 2903 Apr 15 2008 20:34:48 +00:00 cpconfig-8xx.cfg
2 115712 Apr 15 2008 20:34:50 +00:00 home.tar
3 2279424 Apr 15 2008 20:34:54 +00:00 cpexpress.tar
Router#
```

⑤ 要将默认配置文件复制到路由器 NVRAM，输入 copy flash:nvram:命令。

```
Router# copy flash:cpconfig-8xx.cfg nvram:
```

当默认配置文件在 NVRAM 中时，它将成为路由器启动配置。

⑥ 要使新启动配置成为运行中的配置，以便路由器可以支持 Cisco CP，输入 copy

startup-config running-config 命令。

Router# copy startup-config running-config

■ **手动输入配置命令**

如果由于路由器已经有配置或其他原因，不想使用出厂默认配置，则可使用此部分的步骤将每个必要命令添加到配置中。

① 通过控制台端口或以太网端口登录到路由器。

② 如果使用控制台端口，且路由器中没有正在运行的配置，将自动启动 Setup Command Facility，并显示以下文本。

--- System Configuration Dialog ---

Continue with configuration dialog?[yes/no]:

输入 no，然后可以直接输入 Cisco IOS CLI 命令。

如果 Setup Command Facility 没有自动启动，表示有正在运行的配置，应转到下一步。

③ 路由器显示用户 Exec 模式提示符时，输入 enable 命令及其密码（如已配置）。

Router> enable

password password

④ 输入 config terminal 命令进入配置模式。

Router> config terminal

Router(config)#

⑤ 使用以下所示的命令语法，创建具有特权级别 15 的用户帐户。

Router(config)# username name privilege 15 secret 0 password

⑥ 如果路由器接口未配置 IP 地址，配置 IP 地址，以便通过网络访问路由器。以下示例说明已配置快速以太网接口 0。

Router(config)# int FastEthernet0/0

Router(config-if)# ip address 10.10.10.1 255.255.255.248

Router(config-if)# no shutdown

Router(config-if)# exit

如果打算将计算机直接连接到路由器，计算机必须与此接口位于相同子网上。

⑦ 对于非安全通信，将路由器配置为 http 服务器；对于安全通信，则配置为 https 服务器。

要将路由器配置为 http 服务器，输入 ip http server 命令。

Router(config)# ip http server

要将路由器配置为 https 服务器，输入 ip http secure-server 命令。

Router(config)# ip http secure-server

⑧ 输入 ip http authentication local 命令，配置路由器进行本地身份验证。

Router(config)# ip http authentication local

⑨ 配置 http 超时策略。

Router(config)# ip http timeout-policy idle 60 life 86400 requests 10000

⑩ 将 vty 线路配置为特权级别 15。对于非安全访问，输入 transport input telnet 命令。对于安全访问，输入 transport input telnet ssh 命令。

Router(config)# line vty 0 4

```
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

3. 配置计算机 IP 地址

默认配置文件会为路由器上的局域网接口分配 IP 地址，必须将计算机配置为与路由器局域网接口位于相同子网上。如果路由器为固定接口型，表示该路由器已配置为 DHCP 服务器，必须将计算机配置为自动获取 IP 地址。如果路由器可以接受模块化接口，表示该路由器未配置为 DHCP 服务器，必须为计算机配置静态 IP 地址，且该地址与路由器地址位于相同子网上。

先从表 11-3 中找到相应的路由器型号，记下必要的计算机 IP 地址配置。

表 11-3 必要的计算机 IP 地址配置

路由器型号	DHCP 服务器	必要的 IP 地址配置
Cisco 815、Cisco 85x、Cisco 86x、Cisco 87x、Cisco 88x、Cisco 89x、Cisco 180x 和 Cisco 181x	是	自动获取 IP 地址
Cisco 1841、Cisco 1861、Cisco 2800 系列、Cisco 380 系列 0、Cisco 1941、Cisco 2900 系列和 Cisco 3900 系列	否	10.10.10.2～10.10.10.6 的静态 IP 地址，子网掩码为 255.255.255.248

然后，根据需要将计算机的 IP 地址设置为“自动获得 IP 地址”，或者手工指定 IP 地址信息。

4. 将配置计算机连接到路由器

如果要设置新路由器，并想要使用 Cisco CP Express 为路由器设置基本配置，则需要使用跳线将计算机连接到路由器（如图 11-9 所示），以执行初始配置。

对于 Cisco 8xx 系列、Cisco 18xx 系列和 Cisco 19xx 系列路由器而言，可以连接至任意 LAN（或 Switch）接口，对于 Cisco 2800 系列、Cisco 3800 系列、Cisco 2900 系列和 Cisco 3900 系列路由器而言，则需要连接至其 FE 0/0 或 GE 0/0 端口。配置计算机可以连接的路由器以太网接口如表 11-4 所示。

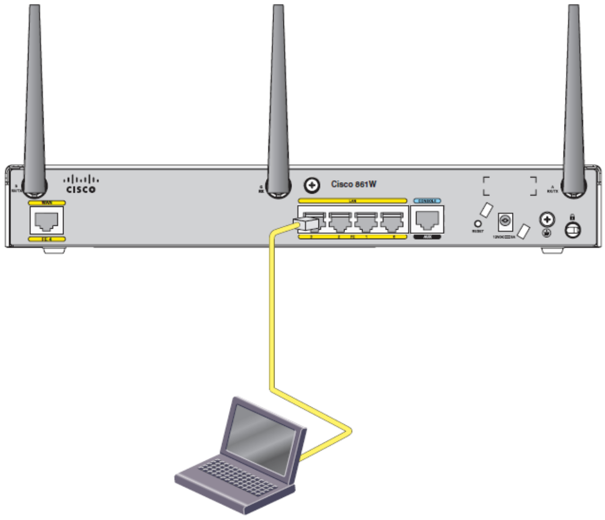
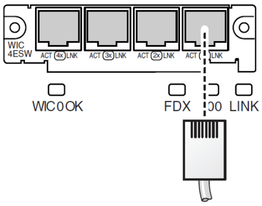
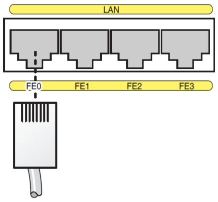
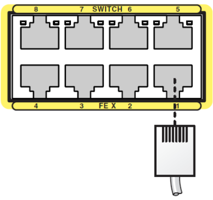
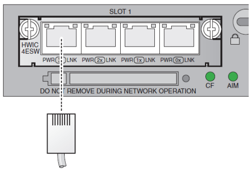
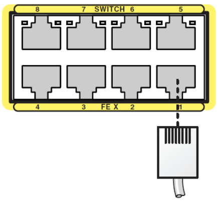
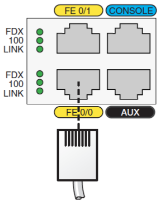
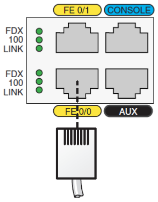
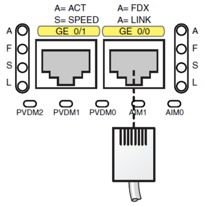
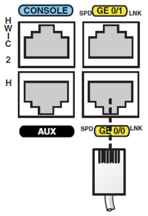
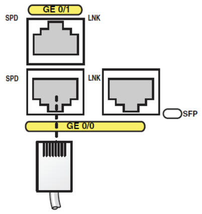
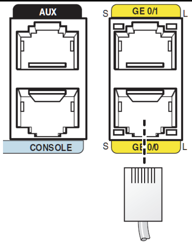
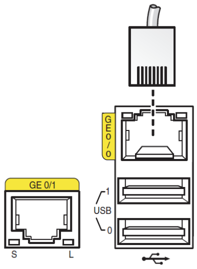


图 11-9　将配置计算机连接到路由器

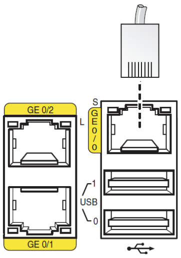
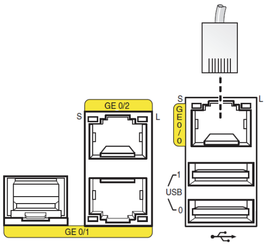
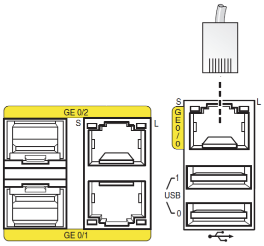
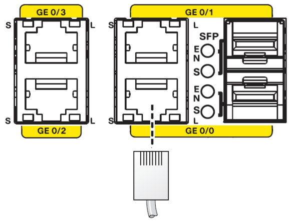
表 11-4　配置计算机连接的路由器以太网接口

路由器型号	电缆类型	将以太网电缆连接至所示端口
Cisco 815	直通	 连接到任一 ACT Lnk 端口
Cisco 850 系列 Cisco 860 系列 Cisco 870 系列 Cisco 880 系列	直通	 连接到任一 LAN 端口
Cisco 1801 Cisco 1802 Cisco 1803	直通	 连接到任一 SWITCH 端口
Cisco 1805	直通	 连接到任一 PWR Lnk 端口

（续表）

路由器型号	电缆类型	将以太网电缆连接至所示端口	
Cisco 1811 Cisco 1812	直通	 连接到任一 SWITCH 端口	
Cisco 1841 Cisco 1861	交叉或直通 （带有以太网交换机）	 连接到 FE 0/0	
Cisco 2800	交叉或直通 （带有以太网交换机）	 连接到 FE 0/0	 连接到 GE 0/0
Cisco 3800	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	 连接到 GE 0/0
Cisco 1905 Cisco 1921	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	
Cisco 2901	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	

（续表）

路由器型号	电缆类型	将以太网电缆连接至所示端口	
Cisco 2911	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	
Cisco 2921 Cisco 2951	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	
Cisco 3925 Cisco 3945	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	
Cisco 3925E Cisco 3945E	交叉或直通 （带有以太网交换机）	 连接到 GE 0/0	

5. 运行 Cisco CP Express 向导

Cisco CP Express 用于快速配置路由器局域网和 Internet 连接。之后，可以使用 Cisco CP 完成更复杂配置。尽管 Cisco CP Express 可用于配置广域网连接、防火墙和安全设置，但是，最好只使用 Cisco CP Express 向导配置以下功能。

- 路由器名称
- 用户名和密码
- 局域网 IP 地址
- DHCP 服务器（如果需要）

① 在计算机上打开 Web 浏览器，禁用任何活动的弹出窗口阻止程序，并输入以下 URL：

http://10.10.10.1

② 在登录页面（如图 11-10 所示）输入用户名 cisco 和密码 cisco。如果启动过程中还出现其他登录页面，输入相同的身份凭证（cisco/cisco）。

图 11-10　登录页面

如果输入 http://10.10.10.1 后没有出现启动页面，执行以下操作来测试计算机和路由器之间的连接。

- 检查路由器上的电源 LED 是否打开，以及连接 PC 的端口的 LED 是否打开，如果都已打开，表示路由器和计算机之间已建立活动以太网连接。如果该 LED 未点亮，请验证是否使用交叉电缆连接计算机和路由器，或者是否使用直通电缆连接路由器和交换机。
- 验证 Web 浏览器的“脱机工作”选项是否已禁用。在 Internet Explorer 中，单击文件菜单，验证是否未选中“脱机工作”选项。
- 验证闪存中是否已加载 cpexpress.tar、home.tar 和 home.shtml 文件。输入用户名 cisco 和密码 cisco，打开与 10.10.10.1 的 Telnet 会话。输入 showflash 命令，显示加载到闪存中的文件。

提·示

出于安全考虑，用户名 cisco 和密码 cisco 将在首次使用后失效。在注销路由器前，必须确保输入“username *username* privilege 15 secret 0 *password* ”命令（将 *username* 和 *password* 替换为要使用的用户名和密码）修改了用户名和密码。此命令创建特权级别为 15 的新用户及相应密码。如果不执行此操作，结束会话后将无法登录路由器。在将来的会话中使用创建的新身份凭证，而不是使用用户名 cisco 和密码 cisco。

- 验证计算机的 IP 地址是否已正确配置。一些路由器要求计算机自动获得 IP 地址，而另一些路由器则要求为计算机配置静态 IP 地址。找到欲配置的路由器，确定计算机的配置方式。

连接到路由器时，会先出现 Cisco CP Express 启动页面（如图 11-11 所示），然后出现一个或多个证书窗口。

图 11-11 Cisco CP Express 启用页面

> **提示**
>
> 所看到的启动页面上的版本号与该版本号可能有所不同。

③ 单击“Yes”（是）或单击“Grant”（同意）接受证书（如图 11-12 所示）。

图 11-12 接受证书

④ 运行“Cisco CP Express Overview”（概述）页面，之后还将运行“Cisco CP Express Wizard”（向导）页面（如图 11-13 所示）。单击“Next”（下一步）按钮开始配置路由器。

> **提示**
>
> Cisco CP Express 向导会要求输入特权加密密码以控制对 Cisco IOS 软件的访问。务必记录或记住您输入的特权加密密码。该密码不会显示在“Enable Password（特权明文密码）”字段或“Summary（摘要）”窗口，如果不擦除路由器配置，也无法重置该密码。此外，还会要求您将路由器的局域网 IP 地址从其默认值更改为其他值。

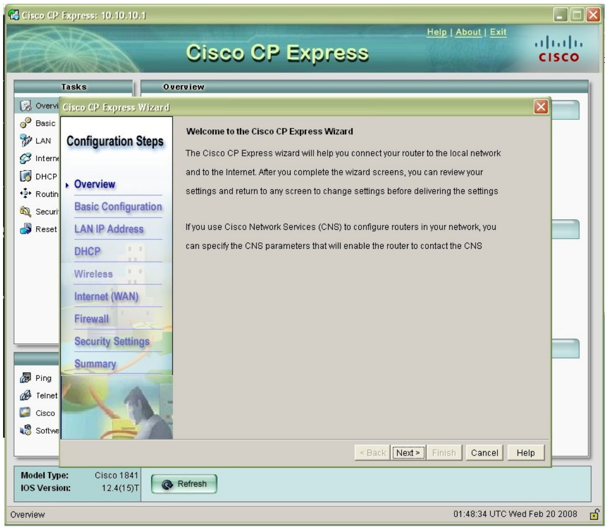


图 11-13　向导页面

⑤ 出现“Summary（摘要）”窗口时，记录输入的局域网 IP 地址、用户名和用户密码，并单击“Finish”（完成）。重新连接路由器以执行其他配置时将需要此信息。

⑥ 退出 Cisco CP Express，用指定给局域网接口的新 IP 地址完成“6. 验证初始配置”，以重新配置计算机并重新连接路由器。

6. 验证路由器初始配置

① 确保计算机 IP 地址与路由器局域网接口的 IP 地址位于相同子网上。

如果是自动获得 IP 地址，在命令行窗口中，先后输入 ipconfig /release 命令和 ipconfig /renew 命令，以从路由器中获取新 IP 地址。输出大致如下所示：

```
C:\> ipconfig /release
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix .: somename.com
IP Address. . . . . . . . . . . . : 0.0.0.0
Subnet Mask . . . . . . . . . . . : 0.0.0.0
Default Gateway . . . . . . . . . :
C:\> ipconfig /renew
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix .: somename.com
IP Address. . . . . . . . . . . . : 192.168.100.168
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.100.1
```

提示　即使计算机原先已配置为自动接受 IP 地址，也必须输入 ipconfig /release 命令和 ipconfig /renew 命令，以释放并重新获得 IP 地址。

如果需要手工为计算机配置静态IP地址，也要保证计算机的IP地址与路由器局域网口的IP地址位于同一子网，并且设置相同的子网掩码。

② 打开Web浏览器，输入为路由器局域网接口指定的新IP地址。

http://新IP地址

例如，如果为局域网接口指定IP地址192.168.100.254，则在浏览器中输入命令http://192.168.100.254。

③ 输入完成Cisco CP Express向导时为路由器指定的用户名和密码。如果显示Cisco CP Express概述窗口（如图11-14所示），证明局域网接口配置有效。

图11-14 概述窗口

④ 通过打开另一个Web浏览器窗口并连接到网站，测试配置的Internet（广域网）连接。如果能够连接到网站（如www.cisco.com），则表示广域网连接正常。如果无法连接，可使用Cisco CP Express或Cisco CP更正广域网设置。

第 12 章　使用 CLI 配置路由器

路由器作为实现不同网络之间互连的关键设备，在局域网远程互连和 Internet 接入中起着非常重要的作用，路由器设置不当将直接影响局域网络与外界的通信，甚至还会埋下网络安全隐患。因此，配置路由器的路由功能，以及路由器的安全功能，无论对于网络互连，还是局域网安全都是至关重要的。

12.1　路由器配置前的准备

路由器基本配置包括以下内容。

- 基本路由器配置
  ① 路由器默认配置
  ② 配置全局参数
- 接口配置
  ① 接口端口
  ② 配置千兆位以太网接口
  ③ 配置无线局域网接口
  ④ 配置接口卡和模块接口
  ⑤ 配置 Loopback 接口
- 路由配置
  ① 配置命令行
  ② 配置静态路由
  ③ 配置动态路由

12.1.1　IP 协议配置原则

为保证 Cisco 路由器在 IP 网络中正常工作，通常遵循图 12-1 所示路由拓扑图的基本规则。

对于路由器 A 和路由器 B 来说，它们互为相邻的路由器。其中，路由器 A 的 S0 与路由器 B 的 S1 为相邻路由器的相邻端口。但是，路由器 A 的 S1 口与路由器 B 的 S0 口不是相邻端口，路由器 A 与路由器 D 也不是相邻路由器。

配置规则如下：

- 路由器的物理网络端口通常要有一个 IP 地址。
- 相邻路由器的相邻端口 IP 地址必须在同一 IP 网络上。
- 同一路由器的不同端口的 IP 地址必须在不同 IP 网段上。
- 除了相邻路由器的相邻端口外，所有网络中路由器所连接的网段即所有路由器的任何

两个非相邻端口都必须不在同一网段上。

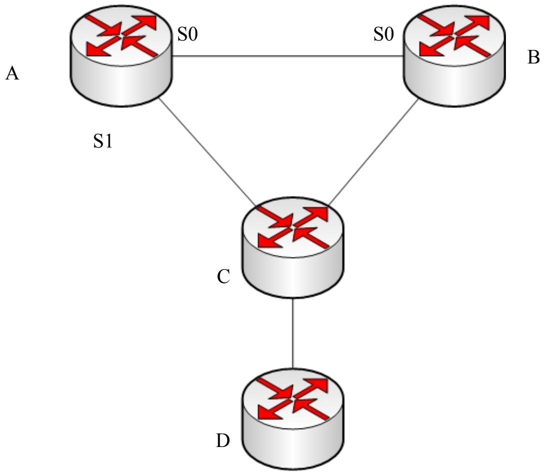


图 12-1　路由拓扑图

12.1.2 路由器默认配置

当第一次引导 Cisco 路由器时，将执行系统默认配置。使用 show running-config 命令，可以查看内置配置。其配置内容大致如下所示。

```
Router# show running-config
Building configuration...
Current configuration : 723 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
!
!
!
```

```
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 3
login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

12.2 路由器基本配置

由于 Cisco CP 的功能相对简单，同时也并不适用于所有的路由器。因此，CLI 配置方式仍然被网络管理员广泛采用。

12.2.1 配置全局参数

需要配置的全局参数主要包括主机名、Enable 密码和禁用域查找，并可为 Cisco 3925E 和 Cisco 3945E 路由器重新分配 I/O 内存。

① 进入全局配置模式。

```
Router> enable
Router# configure terminal
Router(config)#
```

② 为路由器指定主机名。

```
Router(config)# hostname router_name
```

③ 配置 Enable 密码，禁止未授权的访问。

```
Router(config)# enable secret password
```

④ 禁用域查找，避免查找未知词汇的 IP 地址（未知主机名称往往由键入错误所导致）。

```
Router(config)# no ip domain-lookup
```

⑤ 可以重新分配 DRAM 中 I/O 内存和处理器内存所占的百分比。使用 no 命令可以恢复默认内存分配。*i/o-memory-percentage* 值用于分配 DRAM 中用于 I/O 的内存。允许取值为 5、10、15、20、25、30、40 和 50。I/O 内存至少需要 210 MB。

```
Router(config)# memory-size iomem i/o-memory-percentage
```

注·意

推荐配置 I/O 内存所占比例低于 25%，以便于保证 IPSec 的性能。当为 I/O 内存指定所占的百分比后，处理器内存将自动获得 DRAM 中剩余的内存。

12.2.2 配置命令行访问

在路由器初始配置后，可以更为详尽地设置路由器的访问参数，以确保各类访问的安全性和可用性。其中，AUX（Auxiliary，辅助）端口为异步端口，主要用于远程配置，也可借助 Modem 进行拔号连接，支持硬件流控制（Hardware Flow Control）。Console 端口为串行端口，主要用于借助计算机终端进行直接配置。TTY（TeleTYpe）是异步线路用于 Modem 和终端连接的入站和出站，并可以查看路由器或访问服务器配置。VTY（Virtual TYpe terminal，虚拟终

端）是路由器的远程登录的虚拟端口，使用 Telnet 远程进入路由器就是使用的 VTY 口。

① 进入线路配置模式，指定欲配置线路的类型。TTY 线路开始于 3，其他类型的线路开始于 0，并且以 1 为增量递增。需要注意的是，AUX 和 Console 都只能配置一条线路。

```
Router(config)# line [ aux |  console |  tty |  vty ]  line-number
```

如配置 Console 线路

```
Router(config)# line console 0
```

如配置 Telnet 线路，0 4 表示配置 0～4 共 5 条线路，允许 5 台终端同时登录。

```
Router(config)# line vty 0 4
```

② 为该线路指定唯一的密码。

```
Router(config-line)# line password
```

③ 启用密码检查终端登录进程。

```
Router(config-line)# login
```

④ 设置下一次输入命令的等待时间，超时将自动退出登录。默认为 10 分钟。如果设置为 0 0，则永不超时退出。

```
Router(config-line)# exec-timeout  minutes [ seconds ]
```

⑤ 退出线路配置模式，返回特权 EXEC 模式。

```
Router(config-line)# end
Router#
```

12.2.3 配置主机名和密码

当网络中存在有多台路由器时，那么在第一次配置各路由器时，最好对每台路由器都进行命名，以便于与其他路由器区别开来。当然，加密口令（encrypted password）的设置也是必要的，否则，路由器就会成为恶意攻击的对象。

① 进入 Enable 模式，当提示符改变为 Router#时，键入口令。

```
Router> enable
Password: <password>
Router#
```

② 当提示符改变成为 Router（config）#时，即已进入全局配置模式，按 Ctrl+Z 组合键退出该模式。

```
Router# configure terminal
Router(config)#
```

③ 为该路由器命名一个有意义的名字，以取代默认的名称“Router”。

```
Router(config)# hostname xxxx
xxxx(config)#
```

④ 键入新的密钥口令“password”。该口令用于进入特权命令模式。当用户在 Router> 提示符下键入 enable 时，将必须以该口令进行校验，以防止未经授权的用户修改路由器的设置。

```
Router(config)# enable secret password
```

⑤ 进入 Line 配置模式，配置 console 口，防止在一段时间内没有键入而导致与路由器的连接超时，然后再返回至全局配置模式。当进入 line 配置模式时，提示符将改变为 Router（config-line）#。

```
Router(config)# line con 0
Router(config-line)# exec-timeout 0 0
Router(config-line)# end
```

⑥ 校验配置。

```
Router# show running-config
```

⑦ 退出全局配置模式。

```
Router# exit
Router>
```

⑧ 尝试以新口令重新进入。

```
Router> enable
Password: password
Router#
```

⑨ 查看配置。

```
Router# show running-config
```

⑩ 保存配置。如果不保存，在路由器重新启动时，修改的配置将被丢失。

```
Router# copy running-config startup-config
```

12.3 配置物理接口

路由器支持两种类型接口，即物理接口和逻辑接口。物理接口意味着该接口在路由器上有对应的、实际存在的硬件接口，如以太网接口、同步串行接口、异步串行接口、ISDN 接口。逻辑接口意味着该接口在路由器上没有对应的、实际存在的硬件接口，逻辑接口可以与物理接口关联，也可以独立于物理接口存在，如 Dialer 接口、NULL 接口、Loopback 接口、Tunnel 接口、子接口，等等。实际上对于网络协议而言，无论是物理接口还是逻辑接口，都是一样对待的。

12.3.1 接口的一般配置

无论何种类型的端口，通常情况下都可以借助以下操作设置接口的属性，监视接口的状态，禁用或重新启用。

① 指定欲配置的接口，进入指定的接口配置模式。配置每个接口，首先必须进入这个接口的配置模式。首先进入全局配置模式，然后输入以下命令进入指定接口配置模式。

```
Router(config)#interface interface-type interface-number
```

或者，删除指定接口。

```
Router(config)#no interface interface-type interface-number
```

例如，进入千兆以太网口 0/0 端口，步骤是：

```
Router#config terminal
Router(config)#interface gigabitethernet 0/0
```

② 配置 IP 地址和子网掩码。除了 NULL 接口，每个接口都有其 IP 地址，IP 地址的配置是使用接口必须考虑的。

```
Router(config-if)#ip address ip-address ip-mask
```

或者，删除该接口的网络地址。

```
Router(config-if)#no ip address
```

③ 配置接口描述。接口描述用以识别该接口的用途。要配置接口描述，在接口配置模式中执行命令。描述指定接口的用途，最大支持 80 个字符的描述串。

```
Router(config-if)#description interface-description
```

或者，删除该接口用途的描述。

```
Router(config-if)#no description
```

④（可选）配置最大传输单元 MTU。最大传输单元 MTU 是 IP 报文的特性，它的取值范围是 64～65 535 B。

```
Router(config-if)#mtu bytes
```

或者，恢复 MTU 的默认值。

```
Router(config-if)#no mtu
```

⑤（可选）配置带宽 Bandwidth。Bandwidth 主要用于一些路由协议（如 OSPF 路由协议）计算路由量度和 RSVP 计算保留带宽。修改接口带宽不会影响物理接口的数据传输速率。

```
Router(config-if)#bandwidth kilobits
```

或者，取消 bandwidth 的设置。

```
Router(config-if)#no bandwidth
```

⑥ 配置接口发送和接收队列大小。Hold-Queue 用以调整每个接口的发送和接收队列的大小，这个参数可以调整接口处理突发数据的能力。

```
Router(config-if)#Hold-Queue Length {in|out}
```

或者，取消接口队列的设置。

```
Router(config-if)#no Hold-Queue
```

> **提·示** 调整队列大小会增加网络时延，可能会影响实时交互应用。除非觉得有必要，否则不建议修改接口队列大小。

⑦（可选）关闭和重启接口。在需要的时候，接口必须被关闭，比如在接口上更换电缆，然后再重新启动接口。用 shutdown 命令来关闭接口，用 no shutdown 命令来重新启动该接口。

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
```

⑧ 显示接口的传输特性、协议特性的参数，监控接口和控制器状态。

```
Router#Show interface [serial] | [Ethernet] | [FastEthernet]
```

或者，显示接口的当前内部控制寄存器等信息，以及识别到的电缆线等特性。

```
Router#Show controllers [serial] | [Ethernet] | [FastEthernet]
```

> **提·示** 封装不同链路层协议接口的状态，有些内容显示有所不同。

⑨ 清除和复位接口计数。接口上的统计信息随着通信的变化不断地变化，有时为了避免以往通信统计信息的干扰，将接口的统计信息清除，这样，当前的统计信息就可以如实地反映当前接口的通信状况。

将用 show interface 命令显示的接口的通信传输的统计计数值清除为 0。

```
Router#Clear counters [serial] | [Ethernet] | [FastEthernet] | [async]
```

清除某个接口的所有的状态值。

```
Router#Clear interface [serial] | [Ethernet] | [FastEthernet] | [async]
```

⑩ 保存配置。

```
Router # copy runnig-config startup-config
```

12.3.2 配置以太网接口

以太网接口大多用于实现与局域网的连接，因此往往需要配置内部网络的 IP 地址信息。

1. 配置固定以太网接口

① 进入 Enable 模式，在 Router#提示符下键入口令。

```
Router> enable
Password: <password>
Router#
```

② 进入全局配置模式。

```
Router# configure terminal
Router(config)#
```

③ 启用全局模式下的路由协议。该示例中启用 IP 路由。

```
Router# ip routing
```

④ 指定欲配置的快速或千兆以太网端口，进入接口配置模式。

```
Router(config)# interface [ fastethernet | gigabitethernet ] interface-id
Router(config-if)#
```

⑤ 为该接口指定 IP 地址和子网掩码。

```
Router(config-if)# ip address ipaddress sub_mask
```

⑥ 返回至全局配置模式。如果路由器上有多个局域网络接口，重复上述步骤。

```
Router(config-if)# exit
```

⑦ 返回至 Enable 模式。

```
Router(config-if)# end
Router#
```

⑧ 查看配置。

```
Router# show running-config
```

⑨ 保存配置。如果不保存，在路由器重新启动时，修改的配置将被丢失。

```
Router# copy running-config startup-config
```

2. 配置复用以太网接口

如果以太网接口为 SFP 和 RJ-45 复用接口，还应当指定使用哪种类型的接口作为主要接口，或者设置自动备援接口。

以 SFP 为主要接口。

```
Router(config-if)# media-type sfp
```

以 RJ-45 为主要接口。

```
Router(config-if)# media-type rj45
```

同时，还可以指定 SFP 接口作为主要接口，并以 RJ-45 作为自动备援接口。

```
Router(config-if)# media-type sfp auto-failover
```

或者，指定以 RJ-45 作为主要接口，并以 SFP 作为自动备援接口。

```
Router(config-if)# media-type rj45 auto-failover
```

如果没有配置介质类型，可以借助 no media-type 命令启用 Auto-Detect（自动侦测）功能，让路由器自动侦测哪个接口已经连接并启用。如果两个接口都已经连接，那么，先启用的连接将生效。

```
Router(config-if)# no media-type
```

注·意 Auto-Detect 功能只能工作于 1 GigE SFP 接口，而不能侦测 100M SFP。

12.3.3 配置同步串行接口

同步串行口往往用于远程连接，实现与远程网络的通信，因此通常应当配置广域网协议，并配置广域网的 IP 地址信息。

① 进入指定同步串口的配置模式。

```
Router(config)#interface serial serial-number
```

② 设置同步串口的链路封装协议。设置链路封装协议，封装协议是同步串口传输的链路层数据的帧格式，路由器支持 5 种封装协议，即 PPP、帧中继（Frame-Relay）、LAPB、X.25 和 HDLC。同步串口默认值的链路封装格式是 HDLC。

```
Router(config-if)#encapsulation { frame-relay | hdlc | lapb | ppp | x25}
```

③ 设置链路数据压缩传输。链路压缩（也称为按接口的压缩）是对数据包（包括包头和负载）进行整体压缩。它与包头压缩不同，链路压缩是独立于协议的。链路压缩使用 STAC 或者 Predictor 算法来压缩另一链路层（如 PPP 或者 LAPB）上的数据流，以进行差错纠正和数据包排序（在 HDLC 协议上只使用 STAC 压缩），它们都是基于字典的数据压缩技术。Predictor 算法先判断数据是否已经被压缩过。如果数据已经被压缩过，数据会立即被发送出去，而不会浪费时间对已经压缩过的数据进行压缩。STAC 是一种基于 Lempel-Ziv（LZ）的压缩算法。它对每种数据类型只发送一次，然后只发送给各数据类型在数据流中的位置信息。接受方可以使用这些信息重新组装数据流。Predictor 算法是内存密集型的，而 STAC 算法是 CPU 密集型的。也就是说，Predictor 算法比 STAC 算法占用的 CPU 要少，但需要的内存多一些。如果数据流通过点对点连接进行传输，就可以使用链路压缩。在链路压缩环境中，整个数据包都会被压缩，广域网交换网络将无法得到包头中的交换信息。因此，链路压缩适用于有限跳数路径的点对点环境，如专线或者 ISDN。当同步口使用 PPP 或者 HDLC 作为链路封装协议时，可以使用命令

compress stac 实现链路数据压缩传输，从而提供传输效率。

```
Router(config-if)#compress {stac|predictor}
```

提·示　链路数据压缩传输是通过软件实现的，有可能影响系统的整体性能。

或者取消链路数据压缩传输设置。

```
Router(config-if)#no compress [ stac|predictor ]
```

④ 设置线路编解码方式。线路编解码方式有两种，即不归零方式（NRZ）和反向不归零方式（NRZI）。同步串口的默认值线路编解码方式为不归零方式（NRZ）。

设置同步串口使用 NRZI 线路编解码方式。

```
Router(config-if)#nrzi-encoding
```

设置同步串口使用 NRZ 线路编解码方式。

```
Router(config-if)#no nrzi-encoding
```

⑤ 设置同步串口（DCE）时钟速率。同步串口有两种工作方式，即 DTE 和 DCE，不同的工作方式则选择不同的时钟。如果同步串口作为 DCE 设备，需要向 DTE 设备提供时钟；如果同步串口作为 DTE 设备，需要接受 DCE 设备提供的时钟。两个同步串口相连时，线路上的时钟速率由 DCE 端决定，因此，当同步串口工作在 DCE 方式下时，需要配置同步时钟速率，如果作为 DTE 设备使用，则不需配置，其时钟将由 DCE 端提供。默认值情况下，同步串口没有时钟的设置。如果同步串口作为 DTE 设备，路由器系统将禁止配置其时钟速率。

```
Router(config-if)#clock rate clockrate
```

提·示　同步串口的速率设置必须确保物理接口的电缆支持。具体而言，V.24 电缆最高支持 128 Kbps 的速率。

⑥ 设置反转时钟。在某些特殊情况下，时钟在线路上会产生半个周期的时延，这将导致两端设备对接不上或报文被大量丢弃。这时可以将 DTE 侧设备同步串口的接收时钟信号反转以消除时延的影响。如果同步串口作为 DCE 设备，路由器系统将禁止反转时钟。同步串口的默认值速率设置为禁止反转时钟。

```
Router(config-if)#invert txclock
```

或者，取消同步串口（DTE）反转时钟设置。

```
Router(config-if)#no invert txclock
```

提·示 该命令只对某些 DCE 设备提供的时钟信号有效。通常情况下，不需要设置反转时钟。

⑦ 忽略 DCD 信号。默认值状态下，同步串口工作在 DTE 模式下，此时它通过监视 DCD（Data Carrier Detect）信号来检测线路状态变化。相应地这种情况下对端 DCE 设备会发送 DCD 信号来协同工作，当 DTE 端检测到 DCD 信号后就改变同步口的线路状态。在某些情况下，比如 X.21 协议的物理接口在信号线上并没有 DCD 信号，因此可能用 CTS 或者 DSR 来替代，此时就需要使用 ignore-dcd 命令忽略 DCD 信号，也就是允许同步串口不检测线路的载波信号，而依靠检测其他信号来监视线路状态。同步串口的默认值设置为线路必须检测的载波信号。

```
Router(config-if)#ignore-dcd
```

或者，设置线路必须检测线路的载波信号。

```
Router(config-if)#no ignore-dcd
```

⑧ 设置 DTR 脉冲信号时间。当同步串口线路断开（比如由于同步信号丢失导致线路断开，等等），同步串口硬件设置将会被重新设置，在这个期间，DTR（Data Termianl Ready）信号将会处于非激活状态。对于一些以 DTR 信号作为同步依据的特殊设备（如加密或者类似的设备），可以根据需要设置 DTR 在重置期间的脉冲。同步串口的默认值不设置 DTR 脉冲信号时间。

```
Router(config-if)#pulse-time pulse-in-second
```

或者，取消 DTR 脉冲信号时间设置。

```
Router(config-if)#no pulse-time
```

⑨ 设置 MTU。同步串口的最大传输单元（MTU）影响 IP 报文在该接口上传输拆包和组包。MTU 单位为字节，默认值为 1500。

```
Router(config-if)#mtu mtu-size
```

或者，取消 MTU 设置，恢复为默认值 1500。

```
Router(config-if)#no mtu
```

⑩ 同步串口监控和维护。同步串口常用于提供与广域网的接入服务等。通常使用命令 show interfaces serial 及 show controllers serial 监控与维护同步串口。如果在同步串口上封装了链路层协议，还可以使用对应协议的 Debug 命令来考察同步串口的通信情况。

查看指定的同步串口硬件相关状态。

```
Router#show controllers serial [ serial-number ]
```

查看指定的同步串口软件相关状态。

```
Router#show interfaces serial serial-number
```

⑪ 保存配置。

```
Router # copy runnig-config startup-config
```

12.4 配置逻辑接口

逻辑接口是相对物理接口而言的，它是指能够实现数据交换功能但在物理上不存在、需要通过配置来建立的接口。路由器通常提供 5 类逻辑接口：Loopback（回环）接口，NULL（空）接口，Tunnel（隧道）接口，Dialer（拨号）接口，以及子接口。

12.4.1 Loopback 接口配置

Lookback（回环）是一个完全以软件指定的逻辑上的一个端口，它最大的特点就是可以支持所有的平台，并且状态始终 UP（有点类似于计算机的 127.0.0.1）。Lookback 接口的应用大致包括以下几点。

- 作为路由设备的 ID 标识。在 OSPF 等协议中，协议规定根据 RouterID 来选择指派路由器和备份指派路由器，因为 Loopback 端口始终有效，因此我们通常创建一个 Loopback 端口并封装 IP 地址作为路由器的 ID，协议会首先比较 Loopback 端口的 IP 地址大小进行指派路由器的选择，从而实现路由制订。
- 作为路由设备的非直连网段。在 Loopback 端口配置路由器与别的设备的直连网段之外的网段地址，可以在设备之间测试路由，这也是非常有效和方便的一种做法，以检查设备连通性。
- 作为终端访问的地址。由于 Loopback 端口永远不会宕掉，因此用它的端口地址作为别的终端和设备进行 TELNET 访问的地址是比较常用的一种方式。
- 作为“黑洞”处理。因为路由到 Loopback 的包，会被重新路由回路由器的 Loopback 口，并不会被真正地转发，因此也可以被作为一个路由的“黑洞”，现在也有用 Null 端口来实现，可视为回收站。

Loopback 接口配置类似于以太网接口，可以把它看作一个虚拟的以太网接口。

- 配置 loopback 接口。先创建指定接口号的 loopback，如 loopback 0。

```
Router(config)#interface loopback loopback-interface-number
```

然后，就可以像配置以太网接口一样配置 loopback 接口的 IP 地址信息了。

```
Router(config-if)#ip address ip-address subnet_mask
```

- 删除 loopback 接口。由于 loopback 是虚拟的接口，它只在逻辑意义上存在，可以在需要的时候使用 no 命令删除指定的 loopback 接口。

```
Router(config)#no interface loopback loopback-interface-number
```

- 显示 loopback 接口状态。

```
Router#show interfaces loopback loopback-interface-number
```

12.4.2 NULL 接口配置

路由器还提供 NULL（空）的虚拟接口。该虚拟接口仅仅相当于一个可用的系统设备。

NULL（空）永远都处于 UP 状态，并且永远不会主动发送或者接受网络数据，任何发往 NULL 接口的数据包都会被丢弃。既不能在 NULL 接口上配置 IP 地址，也不能在 NULL 接口上封装任何链路层协议。NULL 主要用于防止路由环路，或用于过滤数据包。

进入 NULL 接口配置。

```
Router(config)#interface null 0
```

允许 NULL 接口发送 ICMP 的 unreachable 消息。

```
Router(config-if)#ip unreachables
```

禁止 NULL 接口发送 ICMP 的 unreachable 消息。

```
Router(config-if)#no ip unreachables
```

NULL 接口更多地被用于网络数据流的过滤。如果使用 NULL 接口，可以通过将不希望处理的网络数据流路由给 NULL 接口，而不必使用访问列表，例如：

```
Router(config)#ip route 127.0.0.0 255.0.0.0 null 0
```

由于 NULL 接口在功能上是一个“空”的系统设备，它不会像以太网或者其他接口一样可显示（例如，使用命令 show running-config 是无法看见它的）。同时，作为系统设备是无法使用 no interface null 命令来删除 NULL 接口的。

12.4.3 Tunnel 接口配置

路由器借助 Tunnel（隧道）接口实现隧道功能，允许利用传输协议（如 IP）来传送任意协议的网络数据包。同其他逻辑接口一样，Tunnel 接口也是系统虚拟的接口。Tunnel 接口并不特别指定传输协议或者负载协议，它提供的是一个用来实现标准的点对点的传输模式。由于 Tunnel 实现的是点对点的传输链路，所以，对于每一个单独的链路都必须设置一个 Tunnel 接口。

Tunnel 传输适用于以下情况。

- 允许运行非 IP 协议的本地网络之间通过一个单一网络（IP 网络）通信，因为 Tunnel 接口支持多种不同的负载协议。
- 允许通过单一的网络（IP 网络）连接间断子网。
- 允许在广域网上提供 VPN（virtual private network）功能。

Tunnel 接口配置操作过程如下。

① 创建 Tunnel 接口并接入该接口的配置模式。与其他逻辑接口一样，第一次进入指定的 Tunnel 接口时，就创建了一个 Tunnel 接口。

```
Router(config)#interface tunnel tunnel-number
```

或者，删除已创建的 Tunnel 接口。

```
Router(config)#no interface tunnel tunnel-number
```

② 设置 Tunnel 接口的源地址。一个 Tunnel 接口需要明确配置隧道的源地址和目的地址，为了保证 Tunnel 接口的稳定性，一般将 Loopback 地址作为隧道的源地址和目的地址。在 Tunnel

接口正常工作之前，需要确认源地址和目的地址的连通性。

```
Router(config-if)#tunnel source {ip-address | interface-name interface-number}
```

或者，取消 Tunnel 接口源地址设置。

```
Router(config-if)#no tunnel source
```

③ 设置 Tunnel 接口目的地址。

```
Router(config-if)#tunnel destination { ip-address | host-name }
```

或者，取消 Tunnel 接口目的地址设置。

```
Router(config-if)#no tunnel destination
```

> **提·示** 在同一台路由上，不能使用相同的源地址与目的地址创建两个相同封装模式的 Tunnel 接口。

④ 设置 Tunnel 接口封装格式。Tunnel 接口的封装格式就是 Tunnel 接口的载体协议。Tunnel 接口的默认封装格式是 GRE。当然，用户也可以根据实际使用情况来决定 Tunnel 接口的封装格式。

```
Router(config-if)#tunnel mode { dvmrp | gre | ipip | nos}
```

或者取消 Tunnel 接口封装格式设置，恢复默认值。

```
Router(config-if)#no tunnel mode
```

⑤ 设置 Tunnel 接口校验。有些情况下，需要使用 Tunnel 接口校验来提供数据完整性的保证。默认值情况下，Tunnel 接口不进行校验。

```
Router(config-if)#tunnel checksum
```

或者，取消 Tunnel 接口校验。

```
Router(config-if)#no tunnel checksum
```

⑥ 设置 Tunnel 接口的 Key。设置 Tunnel 接口的 Key 在一定程度上可以确保 Tunnel 接口两端的安全性，同时也可以防范来自外部的恶意探测与攻击。只有在 Tunnel 接口封装格式为 GRE 的情况下，Tunnel 接口的 Key 设置才起作用，因为此时在每一个 GRE 数据包中都会包含设置的 Tunnel 接口 Key。

```
Router(config-if)#tunnel key key-value
```

或者，取消 Tunnel 接口的 Key 设置。

```
Router(config-if)#no tunnel key key-value
```

> **提·示** Tunnel 的两端必须使用相同的 Key 设置才能正常通信。虽然封装格式为 GRE 的时候，每一个 GRE 数据包都包含这个 Key，但是依赖这个 Key 来获得安全保证的企图是欠考虑的。如果设置了 Tunnel 接口 key，那么必须在所在 Tunnel 接口上设置 no ip mroute-cache 才能支持 ip multicast。

⑦ 设置 Tunnel 接口接收规则。

如果负载协议在维护数据包有序方面的功能不足（比如基于 LLC2 的协议），路由器允许设置 Tunnel 接收规则来丢弃接收到的无序数据包。这项设置将有助于实现网络数据包有序传输。

```
Router(config-if)#tunnel sequence-datagrams
```

或者，Tunnel 按序接收设置。

```
Router(config-if)#no tunnel sequence-datagrams
```

> **提·示** 只有在 Tunnel 的封装格式为 GRE 的情况下，该项设置才有效。

⑧ 监控 Tunnel 接口。

显示 Tunnel 接口状态。

```
Router#show interfaces tunnel tunnel-number
```

打开 Tunnel 接口调试开关。

```
Router#debug tunnel
```

关闭 Tunnel 接口调试开关。

```
Router#no debug tunnel
```

12.4.4 Dialer 接口配置

Dialer 接口即拨号接口。路由器支持拨号的物理接口有同步串口与异步串口。路由器中通过逻辑接口 Dialer 实现了 DDR（按需拨号路由）功能。

进入 Dialer 接口配置模式。与其他逻辑接口一样，在第一次进入 Dialer 接口配置模式时即创建一个 Dialer 接口。

```
Router(config)#interface dialer dialer-number
```

删除已创建的 Dialer 接口。

```
Router(config)#no interface dialer dialer-number
```

Dialer 接口的监控与维护，如果在 Dialer 接口上封装了链路层协议，还可以使用对应协议的 Debug 命令来考察通信情况。

```
Router#show interfaces dialer dialer-number
```

12.4.5 子接口配置

所谓子接口，是指从单个物理接口上衍生出来并依附于该物理接口的逻辑接口，允许在单个物理接口上配置多个子接口，并为应用提供了高度灵活性。子接口是在一个物理接口上衍生出来的多个逻辑接口，即将多个逻辑接口与一个物理接口建立关联关系，同属于一个物理接口的若干个逻辑接口在工作时共用物理接口的物理配置参数，但又有各自的链路层与网络层配置参数。

路由器支持子接口的物理接口包括：

- 非交换式以太网接口。
- 封装帧中继的广域网接口。
- 封装 X.25 的广域网接口。

1. 配置以太网口的子接口

路由器提供命令 interface fastethernet 进入以太网子接口配置模式。同其他逻辑接口一样，在第一次进入以太网子接口配置模式时即创建一个以太网子接口，可以使用命令 no interface fastethernet 来删除已创建的以太网子接口。以太网子接口的参数设置参见以太网接口配置，以及 IP 协议配置部分。

进入以太网子接口配置模式。其中，interface-number 为物理接口序号，subinterface-number 为子接口在该物理接口上的序号，两者之间由标号“.”连接。

```
Router(config)#interface fastethernet interface-number.subinterface-number
```

删除已创建的以太网子接口。

```
Router(config)#no interface fastethernet interface-number.subinterface-number
```

2. 配置封装帧中继的广域网接口的子接口

广域网接口在封装了帧中继后，路由器提供命令 interface serial 进入广域网子接口配置模式。同其他逻辑接口一样，在第一次进入广域网子接口配置模式时即创建一个广域网子接口，可以使用命令 no interface serial 来删除已创建的广域网子接口。

进入广域网子接口配置模式。其中，interface-number 为物理接口序号，subinterface-number 为子接口在该物理接口上的序号，两者之间由标号“.”连接，另外，subinterface-number 必须大于 0。

```
Router(config)#interface serial interface-number. subinterface-number [point-to-point | multipoint]
```

删除已创建的广域网子接口。

```
Router(config)#no interface serial interface-number. subinterface-number [point-to-point | multipoint]
```

在封装帧中继的广域网的子接口创建后，可以在子接口上配置自己的 IP 地址、自己的虚电路，以及自己的帧中继地址映射，在子接口上可以配置帧中继协议，以及其他一些在所属物

理接口上的相关参数。

3. 子接口的监控

同其他接口一样，路由器提供命令“show interfaces”查看子接口状态，只不过需要使用子接口所属的物理接口名称与子接口的序号。对于广域网子接口可以使用其封装协议的 debug 命令监控，对于以太网口的子接口对照以太网实施监控。

12.5 配置 PPP 和 MP 协议

PPP（Point-to-Point Protocol，点到点协议）协议是提供在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套的协议包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。PPP 由于能够提供用户验证、易于扩充和支持同异步而获得较广泛的应用。

12.5.1 PPP 和 MP 协议概述

PPP 是为在同等单元之间传输数据包这样的简单链路设计的链路层协议。这种链路提供全双工操作，并按照顺序传递数据包。设计目的主要是用来通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种共通的解决方案。

1. PPP 运行过程

PPP 协议作为最早的路由协议之一，只要求路由器能互相操作，而不提供任何路由选择，这适用于连接两个网，而每个网各自采用不同的路由协议。PPP 协议能在两个路由器之间互相传递数据分组的基本结构信息。

PPP 运行过程如下。

- PPP 在建立链路之前将首先进行 LCP 协商，协商内容包括工作方式是 SP 还是 MP、验证方式和最大传输单元等项目。
- LCP 协商过后就进入了 Establish 阶段，此时 LCP 状态为 opened，表示链路已经建立。
- 如果配置了验证（远端验证本地或者本地验证远端）就进入 Authenticate 阶段，开始 CHAP 或 PAP 验证。
- 如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 closed；如果验证成功就进入 Network 协商阶段（NCP），此时 LCP 状态仍为 opened，而 IPCP 和 IPXCP 状态从 closed 转到 opened。
- NCP 协商支持 IPCP、IPXCP 和 BRIDGECP 协商，IPCP 协商主要包括双方的 IP 地址，IPXCP 协商主要包括双方的网络号和节点号，BRIDGECP 协商主要包括双方的 MAC 地址、MAC 地址类型、生成树和 Bridge 标识。通过 NCP 协商来选择和配置一个或多个网络层协议。每个选中的网络层协议配置成功后，该网络层协议就可通过这条链路发送报文了。
- 该链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些

外部事件。

2. PPP 的验证方式

PPP 支持两种验证方式，即 PAP 和 CHAP。

■ PAP

PAP 是一种简单的明文验证方式。NAS（Network Access Server，网络接入服务器）要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障措施。

PAP 为 2 次握手验证，口令为明文。PAP 验证过程如下。

- 被验证方发送用户名和口令到验证方。
- 验证方根据用户配置查看是否有此用户，以及口令是否正确，然后返回不同的响应。

■ CHAP

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令（challenge），其中包括会话 ID 和一个任意生成的挑战字串（arbitrary challengestring）。远程客户必须使用 MD5 单向哈希算法（one-way hashing algorithm）返回用户名和加密的挑战口令，会话 ID 及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成的一个挑战字符串来防止受到再现攻击（replay attack）。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第 3 方冒充远程客户（remote client impersonation）进行攻击。

CHAP 为 3 次握手验证，口令为密文（密钥）。CHAP 验证过程如下。

- 验证方向被验证方发送一些随机产生的报文。
- 被验证方用自己的口令字和 MD5 算法对该随机报文进行加密，将生成的密文发回验证方。
- 验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。

3. MP 协议

MP 是 Multi-Link PPP 的缩写，是将多个物理链路的 PPP 捆绑在同一个逻辑接口，旨在增加链路的带宽，只要是支持 PPP 的物理链路都可以启用 MP，互相捆绑在同一个逻辑接口 Dialer 口。MP 允许将 IP 等网络层的报文进行碎片处理，将碎片的报文通过多个链路传输，同时到达同一个目的地，以求汇总所有链路的带宽。

MP 的工作过程如下。

PPP 物理链路在协商完 LCP 的一般参数之后，再发起 MP 请求，如果对方的链路支持 MP，并且给出正确的应答，那么将和其他的物理链路共同捆绑到逻辑接口上，进而进行 NCP（比如 IPCP）协商。如果协商成功，所有 MP 的物理链路将都使用同一个逻辑接口的网络地址。

12.5.2 PPP 协议的配置

PPP 协议的配置过程如下。

① 指定欲配置的接口，进入指定的接口配置模式。

```
Router(config)#interface interface-type interface-number
```

② 配置 PPP 协议，首先需要在接口封装 PPP 协议。

```
Router(config-if)#encapsulation ppp
```

去除接口的 PPP 协议的封装。

```
Router(config-if)#no encapsulation ppp
```

③（可选）配置 PPP CHAP 被验证方。CHAP 认证一般有验证方和被验证方，CHAP 的协商由验证方发起，被验证方只发送 PPP 认证用的用户名和口令。默认值情况下，被验证方发送自己的主机名作为 PPP 用户名。

指定 PPP CHAP 验证的主机名。

```
Router(config-if)#ppp chap hostname hostnmae
```

指定 PPP CHAP 验证的密码。

```
Router(config-if)#ppp chap password {0|7} password
```

如果知道验证方 PPP CHAP 所用的主机名，也可以执行以下配置。

指定 PPP CHAP 验证的主机名。

```
Router(config-if)#ppp chap hostname hostnmae
```

为验证方主机名创建用户数据库记录，两端密码要保持一致。

```
Router(config)#username username password {0|7} password
```

提·示 密码的设定有明文输入和密文输入两种，用 0 是非密文输入，用 1 到 7 是密文输入，默认值输入方式为明文输入。与其他厂家设备互连时，只能采用不加密方式输入。如果要配置双向验证，还要增加验证方的配置。

④（可选）配置 PPP CHAP 验证方。PPP CHAP 验证方将主动发起验证，由于需要验证对方路由器发送的用户名和密码的有效性，验证方还需要创建和维护一个本地用户数据库。作为验证方，在用户数据库中需要设置好各个用户名和相应的密码，而用户名即是对方路由器（被验证方）的 PPP 主机名。

启动 PPP 验证，并指定 PPP CHAP 验证方式。

```
Router(config-if)#ppp authentication chap [callin ]
```

取消 PPP CHAP 验证。

```
Router(config-if)#no ppp authentication chap
```

创建用户数据库记录。用户数据库可以是本地数据库，也可以是 AAA 服务器集中管理用户数据库。

```
Router(config)#username username password {0|7} password
```

> **提·示** Callin 是可选的命令选项，设定之后，只有当对方路由器（被验证方）通过拨号网络拨入时才发起 CHAP 验证，对于由本端路由器拨出而建立 PPP 连接则不发起 CHAP 验证。因此，该命令选项不会影响专线 PPP 协商过程。

⑤（可选）配置 PPP PAP 被验证方。

指定 PPP PAP 验证的用户名和密码。

```
Router(config-if)#ppp pap sent-username username password {0|7} password
```

取消 PPP 的 PAP 验证的设定。

```
Router(config-if)#no ppp pap sent-username
```

⑥（可选）配置 PPP PAP 验证方。

设定 PPP 的 PAP 验证方。

```
Router(config-if)#ppp authentication pap [callin]
```

创建用户数据库记录。用户数据库可以是本地数据库，也可以是 AAA 服务器集中管理用户数据库。

```
Router(config)#username username password {0|7} password
```

⑦（可选）配置 PPP 压缩方式。使用 PPP 压缩，有地址和控制域压缩、IP TCP 报头压缩，以及 Stacker 和 Predictor 压缩方式。地址和控制域压缩一般为系统默认值，而 IP TCP 报头压缩其实是 IP 层的压缩。设置 PPP 层压缩命令，一般是因为线路带宽的瓶颈。而 CPU 过载时，不推荐使用 Stacker 或者 Predictor 压缩方式，因为它们本身就要损耗 CPU 资源。

设定 PPP 的压缩方式。Stacker 压缩是基于 Lempel-Ziv（LZ）的压缩算法，它对于每种数据类型只发送一次，然后只发送各数据类型在数据流中的位置信息。接收方可以利用这些信息重新组装数据流。Pridictor 压缩可以先判断数据是否已经被压缩过，如果是数据将立刻发送，而不会浪费时间将已经压缩过的数据进行压缩。

```
Router(config-if)#ppp compression {stacker|predictor} pap
```

或者，取消 PPP 的压缩。

```
Router(config-if)#no ppp compression
```

⑧（可选）配置 PPP 协商参数。PPP 协商时，LCP 和 IPCP 都有超时时间，一旦到了这个超时时间，LCP 将重新发送请求，这个超时时间可以通过命令设定，以便协调和异种设备互连时出现的不一致协商时间。

```
Router(config-if)#ppp negotiation-timeout seconds
```

或者，恢复 PPP 的协商时间为系统的默认值。

```
Router(config-if)#no ppp negotiation-timeout
```

⑨ 返回特权配置模式。

```
Router(config-if)#end
```

⑩ 保存配置。

```
Router # copy runnig-config startup-config
```

12.5.3 MP 协议的配置

路由器的 MP 是在物理接口层上配置 rotary-group，并且捆绑 dialer 逻辑接口实现的。具体配置过程如下。

① 指定欲配置的接口，进入指定的接口配置模式。

```
Router(config)#interface interface-type interface-number
```

② 封装 PPP 链路协议。多链路 PPP 首先是 PPP 协议，所以不论在物理接口或者在逻辑接口上都必须首先封装 PPP 链路协议。

```
Router(config-if)#encapsulation ppp
```

或者，取消 PPP 链路协议的封装。

```
Router(config-if)#no encapsulation ppp
```

③ 配置 dialer in-band。配置多链路，首先必须在串口接口配置层上配置 DDR，要配置 DDR 必须用如下的命令来实现，这是配置 rotary-group 的前提。

```
Router(config-if)#dialer in-band
```

或者，取消 DDR 配置。

```
Router(config-if)#no dialer in-band
```

④ 配置 rotary-group，设定旋转组的组号，将物理接口捆绑到逻辑接口 dialer group-number 上，以实现多链路的绑定。

```
Router(config-if)#dialer rotary-group group-number
```

或者，删除旋转组。

```
Router(config-if)#no dialer rotary-group group-number
```

提·示 rotary-group 的配置必然要用 DDR。所以，如果事先没有配置 dialer in-band，那么配置 dialer rotary-group 时将自动地配置上 dialer in-band。

⑤ 创建逻辑接口 Dialer。设定好旋转组后，必须创建各个物理接口绑定的逻辑接口 dialer。

其接口号必须和旋转组号一致。创建了逻辑接口 dialer 之后，就进入到 dialer 逻辑接口配置层，相应然必须进行封装 PPP 链路协议，配置 ppp multilink，配置拨号过滤规则等配置操作。

```
Router(config)#interface dialer group-number
```

或者，删除逻辑接口 Dialer。

```
Router(config)#no interface dialer group-number
```

> **提・示** 创建逻辑接口 Dialer 时，必须相应地存在着配置好了旋转组号的物理接口，物理接口利用旋转组号和 Dialer 的逻辑接口号一致来维持绑定。如果删除逻辑接口，必须首先删除物理接口上的旋转组。

⑥ 配置 PPP Multilink。设定多链路 PPP 必须在逻辑接口上设置 PPP multilink 命令，用以指定该逻辑接口使用多链路的协商模式。PPP Mulitlink 是在 dialer 逻辑接口层上设定的。

```
Router(config-if)#ppp multilink
```

或者，取消 ppp multilink 协商模式的设定。

```
Router(config-if)#no ppp multilink
```

⑦ 配置拨号过滤规则。逻辑接口上，还必须配置拨号过滤规则，拨号过滤规则功能强大，可以和 ACL 访问控制列表相结合。

```
Router(config-if)#dialer-group group-number
```

或者设定普通的拨号组列表：允许 IP 报文访问。

```
Router(config)#dialer-list group-number protocol ip permit
```

⑧ 返回特权配置模式。

```
Router(config-if)# end
```

⑨ 保存配置。

```
Router # copy runnig-config startup-config
```

12.5.4 PPP 的监控

使用如下的命令可以查看 PPP 协议串口接口的信息。

```
Router# Router#show interface serial interface-number
```

如果 PPP 链路层协商出现问题，可以用如下的命令来调试 PPP 协议。
在 PPP 通信过程中打印报文调试信息。

```
Router#debug ppp packet
```

在 PPP 通信过程中打印协商调试信息。

```
Router#debug ppp negotiation
```

在 PPP 通信过程中打印授权调试信息。

```
Router#debug ppp authentication
```

12.6 配置 HDLC 协议

Cisco 高层数据链路控制（High-Level Data Link Control，HDLC）协议和 ISO HDLC 有所不同。Cisco HDLC 采用 SDLC 的帧格式，支持同步、全双工操作，却不能支持 ISO HDLC 的流量控制，是不可靠的连接，封装该协议后的可靠连接是由上层完成的。Cisco HDLC 具有效率高、实现简单的特点，是点到点链路协议，因此被作为 Cisco 路由器的默认协议，用于实现 Cisco 路由器之间的远程连接。

12.6.1 HDLC 协议概述

高层数据链路控制（HDLC），是一个同步网上传输数据、面向比特的数据链路层协议，它是由国际标准化组织（ISO）根据 IBM 公司的 SDLC（Synchronous Data Link Control）协议扩展开发而成的。

链路控制协议着重于对分段成物理块或包的数据的逻辑传输，块或包由起始标志引导并由终止标志结束，也称为帧。帧是每个控制、每个响应，以及用协议传输的所有信息的媒体的工具。所有面向比特的数据链路控制协议均采用统一的帧格式，不论是数据还是单独的控制信息均以帧为单位传送。

每个帧前、后均有一标志码 01111110，用作帧的起始、终止指示及帧的同步。标志码不允许在帧的内部出现，以免引起歧义。为保证标志码的唯一性但又兼顾帧内数据的透明性，可以采用“0 比特插入法”来解决。该法在发送端监视除标志码以外的所有字段，当发现有连续 5 个“1”出现时，便在其后添插一个“0”，然后继续发后继的比特流。在接收端，同样监视除起始标志码以外的所有字段。当连续发现 5 个“1”出现后，若其后是一个比特“0”则自动删除它，以恢复原来的比特流；若发现连续 6 个“1”，则可能是插入的“0”发生差错变成“1”，也可能是收到了帧的终止标志码。后两种情况，可以进一步通过帧中的帧检验序列来加以区分。“0 比特插入法”原理简单，很适合于硬件实现。

在面向比特的协议的帧格式中，有一个 8 bit 的控制字段，可以用它以编码方式定义丰富的控制命令和应答，相当于起到了 BSC 协议中众多传输控制字符和转义序列的功能。

作为面向比特的数据链路控制协议的典型，HDLC 具有如下特点。

- 协议不依赖于任何一种字符编码集。
- 数据报文可透明传输，用于实现透明传输的“0 bit 插入法”易于硬件实现。
- 全双工通信，不必等待确认便可连续发送数据，有较高的数据链路传输效率。
- 所有帧均采用 CRC 校验，对信息帧进行编号，可防止漏收或重收，传输可靠性高。
- 传输控制功能与处理功能分离，具有较大灵活性和较完善的控制功能。

鉴于以上特点，目前网络设计普遍使用 HDLC 作为数据链路管制协议。

HDLC 工作过程包括协商建立连接、传输报文、超时断连 3 个阶段。

- 协商建立过程：HDLC 每隔 10 s 后互相发送链路探测的协商报文，报文的收发顺序

是由序号决定的，序号失序则造成链路断连。这种用来探询点到点链路是否激活状态的报文称为 KeepAlive 报文。

- 传输报文过程：将 IP 报文封装在 HDLC 层上，数据传输过程中，仍然进行 KeepAlive 的报文协商以探测链路的合法有效。
- 超时断连阶段：当封装 HDLC 的接口连续 10 次无法收到对方对自己的递增序号的确认时，HDLC 协议 Line Protocol 由 UP 向 Down 转变。此时链路处于瘫痪状态，数据无法通信。

12.6.2 HDLC 配置

HDLC 配置非常简单，具体操作如下。

① 指定欲配置的接口，进入指定的接口配置模式。

```
Router(config)#interface interface-type interface-number
```

② 配置接口 HDLC 封装协议。同步口上默认值封装的协议是 HDLC，如果从其他协议改变封装到 HDLC 协议，需使用 encapsulation hdlc 命令指定。

```
Router(config-if)#encapsulation hdlc
```

③ 配置 HDLC KeepAlive 的间隔时间。同步口的 HDLC 可以配置的参数只有 KeepAlive 的间隔时间，默认值是 10 s，可以根据链路的流量来设置这个时间。

```
Router(config-if)#Keepalive seconds
```

④ 返回特权配置模式。

```
Router(config-if)# end
```

⑤ 打开同步口接口的报文调试开关，实现对 HDLC 协议的监控。

```
Router#debug serial interface
```

⑥ 保存配置。

```
Router # copy runnig-config startup-config
```

12.7 配置静态路由和默认路由

中小型局域网络通常只使用一个路由器，实现局域网络与 Internet 或其他网络的互连。因此，链路拓扑相对简单，路由器的设置也不复杂。通常情况下，只需配置好端口，并添加相应的静态路由即可完成路由器的配置。

12.7.1 配置静态路由

通过配置静态路由，可以人为地指定对某一网络访问时所要经过的路径。在网络结构比较简单，并且到达某一网络只有唯一路径时，均采用静态路由。静态路由的效率最高，系统性能占用最少。对于企业网络而言，往往只有一条连接至 Internet 的链路，因此最适合使用静态

路由。

建立静态路由，使用下述 CLI 命令：

```
ip route prefix mask {ip_address | interface_id}
```

① 进入配置模式。

```
Router# configure terminal
```

② 启用 IP 路由。

```
Router(config)# ip routing
```

③ 设置静态路由。其中，prefix 用于指定所要到达的目的网络；mask 用于指定子网掩码；next-hop-ip-address 用于指定下一跳的 IP 地址，即相邻路由器的端口地址；interface-type interface-number 用于指定本地网络接口。

```
Router(config)# ip route prefix mask { next-hop-ip-address | interface-type interface-number [ ip-address ]}
```

④ 返回 Enable 模式。

```
Router#
```

⑤ 保存修改的配置。

```
Router# copy running-config startup-config
```

12.7.2 配置默认路由

① 进入配置模式。

```
Router# configure terminal
```

② 启用 IP 路由。

```
Router(config)# ip routing
```

③ 设置默认路由。该路由的 IP 地址由 ISP 提供。

```
Router(config)# ip default-network network-number
Router(config)# ip route 0.0.0.0 0.0.0.0 default_gateway
Router(config)# ip route prefix mask next-hop-ip-address
```

④ 返回 Enable 模式。

```
Router#
```

⑤ 保存修改的配置。

```
Router# copy running-config startup-config
```

12.8 网络地址转换

网络地址转换（Network Address Translation，NAT）被广泛应用于各种类型的 Internet 接

入方式和各种类型的网络。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。虽然 NAT 也可以借助于某些代理服务器实现，但考虑到运行成本，很多时候都是在路由器上实现。

12.8.1 理解 NAT

随着接入 Internet 计算机数量的不断猛增，IP 地址资源也就愈加显得捉襟见肘。事实上，除了中国教育和科研计算机网（CERNET）外，用户几乎根本申请不到整段的 C 类 IP 地址了。在其他 ISP 那里，即使是拥有几百台的计算机大型网络接入 Internet，分配给用户的也只有几个或十几个 IP 地址。显然，这几个少得可怜的 IP 地址根本无法满足网络用户需求，于是就产生了 NAT 技术。

1. NAT 简介

借助于 NAT，私有（保留）地址的“内部”网络通过路由器发送数据包时，私有地址被转换成合法的 IP 地址，从而只需使用少量 IP 地址（甚至是 1 个），即可实现私有地址网络内所有计算机与 Internet 的通信。也就是说，在网络内的计算机数量大于 ISP 提供的合法 IP 地址时，NAT 就有了自己的用武之地。

NAT 将自动修改 IP 报文头中的源 IP 地址和目的 IP 地址，IP 校验则在 NAT 处理过程中自动完成。有些应用程序将源 IP 地址嵌入到 IP 报文的数据部分中，所以还需要同时对报文进行修改，以匹配 IP 头中已经修改过的源 IP 地址。否则，在报文数据部分嵌入 IP 地址的应用程序就不能正常工作。令人遗憾的是，尽管 NAT 的 Cisco 版本可以处理许多应用，但它毕竟也不是万能的，还是有一些应用无法被支持。表 12-1 列举了 Cisco NAT 支持的和不支持的应用。

表 12-1　Cisco NAT 支持的和不支持的应用

支持的应用	不支持的应用
任何非源和目的的 TCP/UDP 报文	IP 组播
在 IP 报文的数据部分中的 IP 地址	路由表更新
ICMP	DNS 域的迁移
FTP	BOOTP
TCP 上的 NetBIOS（会话服务除外）	Talk，ntalk
RealAudio	SNMP
White Pines CUSeeMe	NetShow
Streamworks	
DNS（“A”和“PTR”查询）	
H.323	
NetMeeting	
VDOLive	
Vxtreme	

2. NAT 的功能

NAT 具有以下主要功能：

- Internet 访问——NAT 使内部私有 IP 地址能够连接至 Intenet。
- 安全——隐藏内部 IP 地址，有效阻止直接来自外部网络的攻击。

- IP 路由解决方案——使用 NAT 时，复用 IP 地址不再是问题。
- 灵活性——可以根据需要随意改变内部使用的 IP 地址，而不会影响外部有效的共有 IP 地址。例如，服务器能够访问 Internet 并被 Internet 访问，可以保持 Internet 使用的 IP 地址不变，而修改服务器使用的内部 IP 地址。

3. NAT 实现方式

NAT 的实现方式有 3 种，即静态转换、动态转换和动态端口地址转换。

静态转换（Static NAT），是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只能转换为某个公用 IP 地址。借助于静态转换，可实现外部网络对内部网络中某些特定设备（如服务器）的访问。

动态转换（Dynamic NAT），是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对是不确定的，是随机的，所有被授权访问 Internet 的私有 IP 地址，可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

动态端口地址转换（Dynamic Port Address Translation，PAT），是指改变外出数据包的源端口并且端口转换完成。采用 PAT 方式，内部网络的所有主机均可共享一个合法外部 IP 地址以实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最为广泛。

4. 网络地址转换的实现

在配置网络地址转换实现的过程之前，首先必须搞清楚内部接口和外部接口，以及在哪个外部接口上启用 NAT。通常情况下，连接到企业网络的接口是 NAT 内部接口，而连接到外部网络（如 Internet）的接口是 NAT 外部接口，如图 12-2 所示。

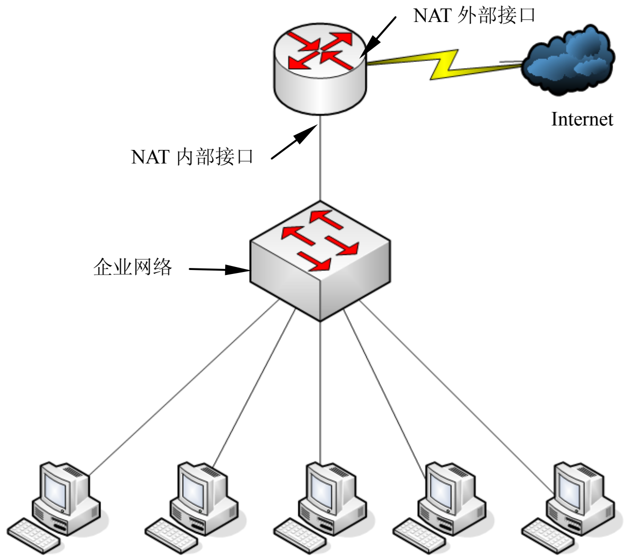


图 12-2　网络地址转换

12.8.2 静态地址转换的实现

所谓静态地址转换，是指将合法 IP 地址一一对应地转换为内部私有 IP 地址。如果企业网络获得了多个合法 IP 地址，可以借助静态地址转换方式，将合法 IP 地址转换为内部服务器的 IP 地址，从而实现对企业网络和 Internet 对服务器的访问。

内部网络使用的 IP 地址段为 192.168.100.1～192.168.100.254，路由器局域网端口（即默认网关）的 IP 地址为 192.168.100.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128～121.17.46.135，路由器广域网中的 IP 地址为 121.17.46.129，子网掩码为 255.255.255.248，可用于转换的 IP 地址为 121.17.46.133。要求将内部网址 192.168.100.2～192.168.100.6 分别转换为合法 IP 地址 121.17.46.133。

① 设置外部端口。

```
interface serial 0/0
 ip address 121.17.46.133 255.255.255.248
 ip nat outside
```

② 设置内部端口。

```
interface fastethernet 0/0
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
```

③ 在内部本地地址与内部合法地址之间建立静态地址转换。

```
ip nat inside source static 内部本地地址内部合法地址
```

示例：

```
ip nat inside source static 192.168.100.2 121.17.46.130
!--将内部网络地址 192.168.100.2 转换为合法 IP 地址 121.17.46.130
ip nat inside source static 192.168.100.3 121.17.46.131
!--将内部网络地址 192.168.100.3 转换为合法 IP 地址 121.17.46.131
ip nat inside source static 192.168.100.4 121.17.46.132
!--将内部网络地址 192.168.100.4 转换为合法 IP 地址 121.17.46.132
ip nat inside source static 192.168.100.5 121.17.46.133
!--将内部网络地址 192.168.100.5 转换为合法 IP 地址 121.17.46.133
ip nat inside source static 192.168.100.6 121.17.46.134
!--将内部网络地址 192.168.100.6 转换为合法 IP 地址 121.17.46.134
```

至此，静态地址转换配置完毕。

12.8.3 动态地址转换的实现

所谓动态地址转换，是指将内部私有 IP 地址动态地转换为合法 IP 地址池内的 IP 地址，对应关系是不固定的。如果企业网络获得多个合法 IP 地址，可以借助动态地址转换方式，实现 Internet 连接共享。

内部网络使用的 IP 地址段为 172.16.100.1～172.16.100. 254，路由器局域网端口（即默认

网关）的 IP 地址为 172.16.100.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128～121.17.46.191，路由器广域网中的 IP 地址为 121.17.46.129，子网掩码为 255.255.255.192，可用于转换的 IP 地址范围为 121.17.46.130～121.17.46.190。要求将内部网址 172.16.100.1～172.16.100.254 动态转换为合法 IP 地址 121.17.46.130～121.17.46.190。

① 设置外部端口。

设置外部端口命令的语法如下：

```
ip nat outside
```

示例：

```
interface serial 0/0
  !--进入串行端口serial 0/0
 ip address 121.17.46.129 255.255.255.248
!--将其IP地址指定为121.17.46.129，子网掩码为255.255.255.248
 ip nat outside
!--将串行口serial 0/0设置为外网端口
!--注意，可以定义多个外部端口
```

② 设置内部端口。

设置内部端口命令的语法如下：

```
ip nat inside
```

示例：

```
interface fastethernet 0/0
!--进入快速以太网端口FastEthernet 0/0
 ip address 172.16.100.1 255.255.255.0
!--将其IP地址指定为172.16.100.1，子网掩码为255.255.255.0
 ip nat inside
!--将FastEthernet 0/0设置为内网端口
!--注意，可以定义多个内部端口
```

③ 定义合法 IP 地址池。

定义合法 IP 地址池命令的语法如下：

```
ip nat pool 地址池名称 起始IP地址 终止IP地址 子网掩码
```

其中，地址池名字可以任意设定。

示例：

```
ip nat pool chinanet 121.17.46.130 121.17.46.190 netmask 255.255.255.192
!--指明地址缓冲池的名称为chinanet，IP地址范围为121.17.46.130～121.17.46.190
!--子网掩码为255.255.255.192。需要注意的是，即使掩码为255.255.255.0
!--也会由起始IP地址和终止IP地址对IP地址池进行限制。
!--或ip nat pool test 121.17.46.130 121.17.46.190 prefix-length 26
```

④ 定义内部网络中允许访问 Internet 的访问列表。

定义内部访问列表命令的语法如下：

```
access-list 标号 permit 源地址 通配符
```

其中，标号为 1～99 之间的整数。

```
access-list 1 permit 172.16.100.0 0.0.0.255
!--允许访问 Internet 的网段为 172.16.100.0～172.16.100.255，主机掩码为 0.0.0.255。
```

需要注意的是，在这里采用的是主机掩码，而非子网掩码。子网掩码与主机掩码的关系为：主机掩码+子网掩码=255.255.255.255。例如，子网掩码为 255.255.0.0，则主机掩码为 0.0.255.255；子网掩码为 255.0.0.0，则主机掩码为 0.255.255.255；子网掩码为 255.252.0.0，则主机掩码为 0.3.255.255；子网掩码为 255.255.255.192，则主机掩码为 0.0.0.63。

另外，如果想将多个 IP 地址段转换为合法 IP 地址，可以添加多个访问列表。例如，当欲将 172.16.98.0～172.16.98.255 和 172.16.99.0～172.16.99.255 转换为合法 IP 地址时，应当添加下述命令。

```
access-list 2 permit 172.16.98.0 0.0.0.255
access-list 2 permit 172.16.99.0 0.0.0.255
```

⑤ 实现网络地址转换。

在全局设置模式下，将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。命令语法如下：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字
```

示例：

```
ip nat inside source list 1 pool chinanet
```

如果有多个内部访问列表，可以一一添加，以实现网络地址转换，如：

```
ip nat inside source list 2 pool chinanet
ip nat inside source list 2 pool chinanet
```

至此，动态地址转换设置完毕。

12.8.4 动态端口地址转换

所谓动态端口地址转换，是指通过复用 TCP 端口的方式，使用一个合法 IP 地址实现 Internet 连接共享。如果企业网络只获得一个合法的 IP 地址，则应当采用动态端口地址转换方式。

内部网络使用的 IP 地址段为 10.100.100.1～10.100.100.254，路由器局域网端口（即默认网关）的 IP 地址为 10.100.100.1，子网掩码为 255.255.255.0。路由器广域网中的 IP 地址为 202.99.160.1，子网掩码为 255.255.255.248。要求将内部网址 10.100.100.1～10.100.100.254 转换为合法 IP 地址。

① 进入全局配置模式。

```
Router# config term
```

② 设置外部端口。

```
Router(config)# interface serial 0/0
Router(config-if)# ip address 202.99.160.1 255.255.255.252
Router(config-if) # ip nat outside
```

③ 返回全局配置模式。

```
Router(config-if) # exit
```

④ 设置内部快速以太网端口。

```
Router(config)# interface fastethernet 0/0
Router(config-if) # ip address 1.100.100.1 255.255.255.0
Router(config-if) # ip nat inside
```

⑤ 返回全局配置模式。

```
Router(config-if) # exit
```

⑥ 设置复用动态地址转换，复用串行口合法 IP 地址。

```
Router(config)# ip nat inside source list 120 interface Serial0/0 overload
!--指明复用串行口的合法 IP 地址，访问列表为 120
```

⑦ 定义内部访问列表。

```
Router(config)# access-list 120 permit ip 10.100.100.1.0 0.0.0.255 any
!—定义 120 访问列表，允许访问 Internet 的网段为 10.100.100.0～10.100.100.255
!--子网掩码为 255.255.255.0，主机掩码为 0.0.0.255
```

在全局设置模式下，设置在内部的本地地址与内部合法 IP 地址间建立复用动态地址转换。命令语法如下：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字 overload
```

示例：

```
ip nat inside source list 1 pool public overload
!--以端口复用方式，将访问列表 1 中的私有 IP 地址转换为
!--public IP 地址池中定义的合法 IP 地址
```

⑧ 返回 Enable 模式。

```
Router(config)# end
```

⑨ 保存配置。

```
Router# running-config startup-config
```

至此，端口复用动态地址转换完成。

12.9 配置 RIP

RIP（Routing Information Protocol）路由协议是一种相对古老，在小型及同介质网络中得到了广泛应用的路由协议。RIP 采用距离向量算法，是一种距离向量协议。RIP 在 RFC 1058 文档中定义。

RIP 使用 UDP 报文交换路由信息，UDP 端口号为 520。通常情况下 RIPv1 报文为广播报文；而 RIPv2 报文为组播报文，组播地址为 224.0.0.9。RIP 每隔 30 s 向外发送一次更新报文。如果路由器经过 180 s 没有收到来自对端的路由更新报文，则将所有来自此路由器的路由信息

标志为不可达，若在 240 s 内仍未收到更新报文就将这些路由从路由表中删除。

RIP 使用跳数来衡量到达目的地的距离，称为路由量度。在 RIP 中，路由器到与它直接相连网络的跳数为 0；通过一个路由器可达的网络的跳数为 1，其余依此类推；不可达网络的跳数为 16。

12.9.1 RIP 的默认配置

表 12-2 显示了 RIP 的默认设置。

表 12-2　RIP 的默认设置

特　　性	默认设置
自动摘要(Auto summary)	启用
初始默认信息	无
默认 metric	Built-in;自动翻译
IP RIP 认证关键链	未认证 认证模式：clear text.（清除文本）
IP RIP 接收版本	依路由器配置命令版本
IP RIP 发送版本	依路由器配置命令版本
IP RIP triggered	依路由器配置命令版本
IP split horizon	使用媒体分类(varies with media)
相邻近（neighbor）	未定义
网络	未指定
Offset list	禁用
输出延迟	0 ms
基本时钟	更新：30 s 无效：180 s Hold-down：180 s Flush：240 s
无效更新源	禁用
版本	接收 RIP 版本 1 和版本 2 数据包；发送版本 1 数据包

12.9.2 配置 RIP 路由

若欲配置 RIP 路由，必须为一个网络启用 RIP 路由器，并且选择性地配置一些相关参数。在特权 Exec 模式下开始，启用并且配置 RIP。

① 进入全局配置模式。

```
Router # configure terminal
```

② 启用 IP 路由器。

```
Router (config) # ip routing
```

③ 启用 RIP 路由器，进入路由器配置模式。

```
Router (config) # router rip
```

④ 使用 RIP 路由器程序连接一个网络。

```
Router (config) # network network number
```

⑤（可选）定义一个相邻路由器，以交换路由信息至该路由器。

```
Swtich (config) # neighbor ip-address
```

⑥（可选）偏移量设置，是对通过 RIP 学习和通告的路由进行路由量度的增加设置。通过应用匹配访问列表，可以对某个指定接口的某些进站和出站路由进行偏移量设置，而其他路由偏移量保持不变。

```
Router (config) # offset list [access-list number | name] {in |out} offset [type number]
```

提·示 设置 RIP 偏移量，需要注意当量度值为 16 时，该路由将被看作无效路由，此偏移量的取值十分重要。偏移量设置适当，也可以用于过滤路由。

⑦（可选）调整路由协议时钟。update——路由更新时间，定义路由器发送路由更新报文的周期，默认为 30 s。invalid——路由无效时间，定义路由表中路由因没有更新而变为无效的时间，默认为 180 s。holddown——路由拒绝时间，在该时间内，路由器不会接受其他路径的路由，默认为 180 s。flush——路由清除时间，该时间过后，该路由将被清除出路由表，默认为 240 s。

```
Router (config) # timers basic update invalid holddown flust
```

提·示 通过调整以上时钟，可能会加快路由协议的收敛时间及故障恢复时间。

⑧（可选）配置接收和发送 RIP 版本 1 或者 RIP 版本 2 数据包。默认情况下，只接收版本 2 发送版本 1。

```
Router (config) # version {1|2}
```

⑨（可选）禁用自动汇总。RIP 路由自动汇总，就是当子网路由穿越有类网络边界时，将自动汇总成有类网络路由。RIPv2 默认值情况下将进行路由自动汇总，RIPv1 不支持该功能。RIPv2 路由自动汇总的功能，提高了网络的伸缩性和有效性。如果有汇聚路由存在，在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模。

通告汇聚路由会比通告单独的每条路由更有效率，主要有以下因素。

- 当查找 RIP 数据库时，汇聚路由会得到优先处理。
- 当查找 RIP 数据库时，任何子路由将被忽略，减少了处理时间。

有时可能希望学到具体的子网路由，而不愿意只看到汇总后的网络路由，这时需要关闭路由自动汇总功能。

```
Router (config) # no auto summary
```

⑩（可选）禁止 RIP 路由源地址验证配置。默认情况下，RIP 会对进站的路由更新报文源地址进行验证，如果源地址无效，RIP 就会丢弃该报文。判断源地址是否有效，就是判断源 IP 地址是否与接口 IP 地址在相同的网络内。如果是无编号 IP 地址接口，将不会进行有效性验证。

```
Router (config) # no validate-update-source
```

⑪（可选）增加 RIP 更新发送延迟。

```
Router (config) # output-delay delay
```

⑫ 返回特权 Exec 模式。

```
Router (config-router) # end
```

⑬ 校验配置。

```
Router # show ip protocols
```

⑭ 保存配置。

```
Router # copy running-config startup-config
```

禁用 RIP 路由时，使用“**no router rip**”全局配置命令。

若欲显示活动路由器协议的参数和目前的状态，使用“**show ip protocols**”特权 Exec 命令。使用“**show ip rip database**”特权 Exec 命令可显示 RIP 数据库中的地址。

12.9.3 配置 RIP 认证

RIP 版本 1 不支持认证。如果发送并接收 RIP 版本 2 数据包，可以在接口上启用 RIP 认证。路由器支持两种认证的模式，即明文认证和 MD5 认证。默认为明文认证方式。

在特权 Exec 模式下开始，在接口上配置 RIP 认证。

① 进入全局配置模式。

```
Router # configure terminal
```

② 进入接口配置模式，并且指定欲配置的接口。

```
Router (config) # interface interface-id
```

③ 启用 RIP 认证。

```
Router (config) # ip rip authentication key-chain name-of-chain
```

④ 配置接口来使用明文认证或者 MD5 认证。

```
Router (config) # ip rip authentication mode [text |md5]
```

⑤ 返回特权 Exec 模式。

```
Router (config-router) # end
```

⑥ 校验配置。

```
Router # show running-config interface [interface-id]
```

⑦ 保存配置。

```
Router # copy running-config startup-config
```

重新清除明文认证，使用“**no ip rip authentication mode**”接口配置命令。若欲禁用认证，使用“**no ip rip authentication key-chian**”接口配置命令。

12.9.4 配置水平分割

多台路由器连接在 IP 广播类型网络上，又运行距离向量路由协议时，就有必要采用水平分割的机制以避免路由环路的形成。水平分割可以防止路由器将某些路由信息从学习到这些路由信息的接口通告中出去，这种行为优化了多个路由器之间的路由信息交换。

然而，对于非广播多路访问网络（如帧中继、X.25 网络），水平分割可能造成部分路由器学习不到全部的路由信息。在这种情况下，可能需要关闭水平分割。如果一个接口配置了 IP 地址，也需要注意水平分割的问题。

> **提·示** 封装帧中继时，接口默认值为关闭水平分割；帧中继子接口、X.25 封装默认值为打开水平分割；其他类型的封装默认值均为打开水平分割。因此，在使用中一定要注意水平分割的应用。

1. 配置命令

① 进入全局配置模式。

```
Router # configure terminal
```

② 进入接口配置模式，并指定欲配置的三层接口。

```
Router (config) # interface interface-id
```

③ 配置 IP 地址和 IP 子网。

```
Router (config-if) # ip address ip-address subnet-mask
```

④ 配置 RIP 汇总 IP 地址信息。

```
Router (config-if) # ip summary-address rip ip address ip-network mask
```

⑤ 在接口上禁用水平分割。

```
Router (config) # no ip split horizon
```

⑥ 返回特权 Exec 模式。

```
Router (config-router) # end
```

⑦ 校验配置。

```
Router # show ip interface interface-id
```

⑧ 保存配置。

```
Router # copy runnig-config startup-config
```

禁用 IP 汇总，使用“**no ip summary-address rip**”路由器配置命令。

2. 配置示例

在该示例中，major 网络为 10.0.0.0，汇总地址为 10.2.0.0，自动汇总地址为 10.0.0.0。所以，10.2.0.0 在出口 Gigabit Ethernet 2 上被广告，10.0.0.0 不被广告。在该示例中，如果接口仍然处于 2 层模式，必须键入 no switchport 接口配置命令，使其成为三层接口，然后，才能为其指定 IP 地址信息。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

12.10 配置 OSPF

OSPF（Open Shortest Path First）是为 IETF OSPF 工作组开发的一种基于链路状态的内部网关路由协议。OSPF 是专为 IP 开发的路由协议，直接运行在 IP 层上面，协议号为 89，采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5（全部 OSPF 路由器）和 224.0.0.6（指定路由器）。

12.10.1 默认的 OSPF 配置

表 12-3 显示的是 OSPF 的默认配置。

表 12-3　OSPF 的默认配置

特　　性	默认设置
接口参数	Cost: 无默认配置 Retransmit interval: 5 s Transmit delay: 1 s Priority: 1 Hello interval: 10 s Dead interval: hello interval 的 4 倍 没有认证 没有指定的密码 MD5 认证禁用
区域	Authentication type: 0 Defalut cost: 1 Range:禁用 Stub:无定义 NSSA:无定义
自动 cost	100 Mbps

（续表）

特　性	默认设置
默认初始信息	禁用。当启用时，默认设置为 10，并且外部路由器类型默认为类型 2
默认 Metric 值	建立
远程 OSPF	Dist1:110 Dist2:110 Dist3:110
OSPF 数据库过滤器	禁用
IP OSPF 名称查询	禁用
Log adjacency changes	启用
相邻	未定义
相邻数据库过滤器	禁用
网络区域	禁用
NSF awareness	启用
路由器 ID	没有指定 OSPF 路由程序
总地址	禁用
LSA 组速率时钟	240 s
最短路径时钟	Spf:5 s Spf 延迟时间：10 s
虚拟连接	未指定区域 ID 或路由器 ID Hello interval:10 s Retransmit interval:5 s Transmit delay:1 s Dead interval: 40 s Authenticatin key:无 Message-digest key:无

12.10.2 配置基本 OSPF 参数

创建 OSPF 路由进程，并定义与该 OSPF 路由进程关联的 IP 地址范围，以及该范围 IP 地址所属的 OSPF 区域。OSPF 路由进程只在属于该 IP 地址范围的接口发送、接收 OSPF 报文，并对外通告该接口的链路状态。

在特权 Exec 模式下开始，启用 OSPF。

① 进入全局配置模式。

```
Router # configure teminal
```

② 启用 OSPF 路由器，并进入路由器配置模式。

```
Router (config) # router ospf process-id
```

③ 指定 OSPF 运行的接口和接口的区域 ID。Network 命令中 32 个“比特通配符”与掩码的取值相反，取“1”代表不比较该比特位，“0”代表比较该比特位。不过用掩码的方式来定义，路由器也会自动翻译成比特通配符。只要接口地址与 Network 命令定义的 IP 地址范围相匹配，该接口就属于指定的区域。

```
Router (config-router) # network address wildcard-mask area area-id
```

④ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑤ 校验配置。

```
Router # show ip protocols
```

⑥ 保存配置。

```
Router # copy running-config startup-config
```

若欲终止 OSPF 路由进程，使用“**no router ospf** *process-id*”全局配置命令。

12.10.3 配置 OSPF 接口

使用“**ip ospf**”接口配置命令，可以更改指定接口的 OSPF 参数。应该注意的是，一些参数的设置必须保证与该接口相邻接的路由器的相应参数一致。

在特权 Exec 模式下开始，修改 OSPF 接口参数。

① 进入全局配置模式。

```
Router # configure teminal
```

② 进入接口配置模式，并指定欲配置的三层接口。

```
Router (config) # interface interface-id
```

③（可选）在接口上精确地指定发送数据包的费用。

```
Router (config) # ip ospf cost
```

④（可选）指定 OSPF 链路状态通告重传时间间隔。

```
Router (config) # ip ospf retransmit-intervaln seconds
```

⑤（可选）设置 OSPF 发送一个更新报文的时间。

```
Router (config) # ip ospf transmit-delay seconds
```

⑥（可选）设置 OSPF 优先值，用于指定路由器。

```
Router (config) # ip osfp priority number
```

⑦（可选）设置发送 HELLO 报文时间间隔。

```
Router (config) # ip osfp hello-interval seconds
```

⑧（可选）设置无效时间间隔，在该时间内如果没接收到邻居的 HELLO 报文，则宣告邻居无效。

```
Router (config) # ip ospf dead-interval seconds
```

⑨（可选）设置 OSPF 明文认证密钥。

```
Router (config) # ip ospf authentication-key key
```

⑩（可选）设置 OSPF MD5 认证密钥。

```
Router (config) # ip ospf message digest-key keyid md5 key
```

⑪（可选）在该接口阻塞 OSPF LSA 包泛洪。

```
Router (config) # ip ospf database-filter all out
```

⑫ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑬ 显示 OSPF 接口信息。

```
Router # show ip ospf interface [interface-name]
```

⑭ 显示相邻路由器的 NSP 状态。

```
Router # show ip ospf neighbor detail
```

⑮ 保存配置。

```
Router # copy running-config startup-config
```

使用这些命令的“**no**”形式移除已配置的参数值或返回默认值。

12.10.4 配置 OSPF 区域参数

当需要配置区域认证、残域、默认值汇总路由花费时，就需要通过配置区域命令来实现。配置区域认证是为了防止学到非认证、无效路由，以及避免通告有效路由到非认证路由器，在广播类型网络中，区域认证还可以避免非认证路由器成为指定路由器的可能性，保证了路由系统的稳定性和抗入侵性。

当一个区域为 OSPF 路由域的叶区域，即该区域不作为过渡区域，也不会向 OSPF 路由域注入外部路由时，可以考虑将该区域配置为残域（Stub Area）。残域路由器只能学到 3 种路由，一是残域内部路由，二是其他区域路由，三是残域边界路由器通告的默认值路由。由于没有大量的外部路由，所以残域路由器的路由表将很小，可以节约路由器的资源，因此残域的路由器可以为中低端设备。

如果配置了全残域，残域路由器就只能学到 2 种路由，一是残域内部路由，二是残域边界路由器通告的默认路由。全残域的配置，使得 OSPF 占用路由器资源最小化，提高了网络传输效率。

如果残域路由器可以学到多条默认值路由，就需要对默认路由的花费进行设置，这样就可以控制残域路由器优先使用指定的默认值路由。

在特权 Exec 模式下开始，配置区域参数。

① 进入全局配置模式。

```
Router # configure teminal
```

② 启用 OSPF 路由，并进入路由器配置模式。

```
Router (config-router) # router ospf process-id
```

③（可选）区域认证方式设置为明文认证。

```
Router (config) # area area-id authentication
```

④（可选）区域认证方式设置为 MD5 认证。

```
Router (config) # area area-id authentication message-digest
```

⑤（可选）将区域设置为残域或全残域。

```
Router (config) # area area-id stub [no-summary]
```

⑥（可选）为广告路由器指定地址范围。

```
Router (config) # area area-id range address mask
```

⑦ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑧ 查看 OSPF 路由进程相关信息。

```
Router # show ip ospf [process-id]
```

⑨ 查看指定路由器 OSPF 的数据库信息。

```
Router # show ip ospf [process-id [area-id]] database
```

⑩ 保存配置。

```
Router # copy running-config startup-config
```

使用这些命令的“**no**”形式移除已配置的参数值或返回默认值。

12.10.5 配置其他 OSPF 参数

在特权 Exec 模式下开始，配置其他的 OSPF 参数。

① 进入全局配置模式。

```
Router # configure terminal
```

② 启用 OSPF 路由，并进入路由配置模式。

```
Router (config-router) # router ospf process-id
```

③（可选）配置外部汇聚路由。当路由从其他路由进程重新分布，注入 OSPF 路由进程时，每条路由均分别单独以一个外部链路状态的方式通告给 OSPF 路由器。如果注入的路由是一个连续的地址空间，自治域边界路由器也可以只通告一个汇聚路由，从而大大减小路由表的规模。

```
Router (config) # summary-address address mask
```

④（可选）创建虚拟连接。在 OSPF 路由域中，所有的区域都必须与骨干域连接，如果骨干域断接，就需要配置虚拟链接将骨干域接续起来，否则网络通信将出现问题。虚拟链接需要在两个区域边界路由器（ABR）之间创建，两个 ABR 共同所属的区域称为过渡区域。残域（Stub Area）是不能作为过渡区域的。虚拟链接也可以用于续接其他非骨干区域。

```
Router (config) # area area-id vitual-link router-id [hello-interval seconds] [retransmit-interval seconds] [trans] [[authentication-key key] | message-digest-key keyid md5 key]
```

⑤（可选）产生默认路由。一个自治域系统边界路由器（ASBR），可以强迫其产生一条

默认值路由注入到 OSPF 路由域中。如果一个路由器强制产生默认值路由，该路由器就自动成为 ASBR。但是，ASBR 不会自动产生默认路由的，因此必须强制 ASBR 产生默认路由。

```
Router (config) # default-information originate [always] [metric metric-vlaue] [metric-type type-value] [route-map map-name]
```

提·示 当配置残域时，区域边界路由器将自动产生默认路由，然后通告到残域中的所有路由器。

⑥（可选）配置 OSPF 域名解析。当有关于 OSPF 的状态信息显示时，会尽量以域名的方式标明路由器。路由器以域名的方式显示会更直观方便。

```
Router (config) # ip ospf name-lookup
```

⑦（可选）为将广告的路由器指定地址范围。

```
Router (config) # ip auto-cost reference-bandwidth ref-bw
```

⑧（可选）修改 OSPF 远程值。

```
Router (config) # distance ofsp {[inter-area dist1] [inter-area dist2] [externam dist3]}
```

⑨（可选）在指定接口抑制发送 HELLO 包。

```
Router (config) # passive-interface type number
```

⑩（可选）配置路由计算时间。

```
Router (config) # timers throttle spf spf-delay spf-holdtime spf-wait
```

⑪（可选）当相邻状态改变时，发送 syslog 消息。

```
Router (config) # ospf log-adj-changes
```

⑫ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑬ 显示指定路由器 OSPF 数据库相关信息。

```
Router # show ip ospf [process-id [area-id]] database
```

⑭ 保存配置。

```
Router # copy running-config statup-config
```

12.10.6 配置 Loopback 接口

OSPF 路由进程总是用最大的接口 IP 地址作为路由器标识符，如果该接口关闭或者该 IP

地址不存在了，OSPF 路由进程必须重新计算路由标识符并发送所有的路由信息给邻居。

如果配置了 Loopback（本地环路地址），则路由进程会选择 Loopback 接口的 IP 地址作为路由器标识符；如果有多个 Loopback 接口，则选择 IP 地址最大的地址作为路由器标识符。由于 Loopback 地址会永久存在，增强了路由表的稳定性。

从特权 Exec 模式开始，配置 Loopback 接口。

① 进入全局配置模式。

```
Router # configure terminal
```

② 创建一个 Loopback 接口，并进入接口配置模式。

```
Router (config) # interface loopback 0
```

③ 为 Loopback 接口指定 IP 地址。

```
Router (config-if) # ip address address mask
```

④ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑤ 校验配置。

```
Router # show ip interface
```

⑥ 保存配置。

```
Router # copy running-config startup-config
```

使用“**no interface loopback 0**”全局配置命令来禁用 loopback 接口。

12.10.7 监控 OSPF

借助以下命令，可以查看 OSPF 路由的一些相关信息，便于实现对 OSPF 路由运行状态的监控。

查看 OSPF 路由的基本信息。

```
show ip ospf [process-id]
```

查看与 OSPF 数据库相关的信息。

```
show ip ospf [process-id] database [router] [link-state-id]
show ip ospf [process-id] database [router] [self-originate]
show ip ospf [process-id] database [adv-router] [ip-address]
show ip ospf [process-id] database [network] [link-state-id]
show ip ospf [process-id] database [router] [link-state-id]
show ip ospf [process-id] database [asbr-summary] [link-state-id]
show ip ospf [process-id] database [external] [link-state-id]
show ip ospf [process-id area-id] database [database-summary]
```

查看内部 OSPF 路由 ABR 和 ASBR 表记录。

```
show ip ospf border-routes
```

查看 OSPF 接口信息。

```
show ip ospf interface [interface-name]
```

查看 OSPF 相邻接口信息。

```
show ip ospf neighbor [interface-name] [neighbor-id] detail
```

查看 OSPF 虚拟连接信息。

```
show ip ospf virtual-links
```

12.11 配置 EIGRP

EIGRP 可以使路由器交换信息比使用早先的网络协议更加有效。使用 EIGRP 协议，一个路由器保持一份它的邻近路由器的路由表副本。如果它不能从这些表中找到一条到达目的地的路由，它将向它的邻近路由器询问一个路由并且它们轮流询问它们邻近的路由器直到找到一个路由。为了保持所有的路由器注意邻近路由器的状态，每个路由器定时发出“握手”信息包。一个在一定时间间隔内没有收到“握手”信息包的路由器被认为是无效的。

12.11.1 默认的 EIGRP 配置

表 12-4 为 EIGRP 的默认配置。

表 12-4 EIGRP 默认配置

特　性	默认设置
自动总计	启用
默认信息	在两个 EIGRP 进程之间，外部路由器被接收并且默认信息被通过
默认 Metric 值	只有连接的路由器和接口静态路由器在无默认度量值情况下可以分配 带宽：0 或最大速率（bps） 延迟：0 或 39.1 的任意倍数 可靠性：0～255 的任意数（255 意味着 100%的可靠性） 负载：用 0～255 表示有效带宽（255 意味着 100%的负载） MTU：路由器能够提供的最大传输单元，0 或任意正数
距离	内部距离：90 外部距离：170
EIGRP log-neighbor 改变	禁用
IP 认证 key-chain	不提供
IP 认证模式	不提供
IP 带宽比例	50%
IP hello 间隔	对低速网络 NBMA 来说 60 s；所有其他网络：5 s
IP 挂起时间	对低速 NBMA 网络来说：180 s；其他网络：15 s
IP 水平	启用
IP 总体地址	无定义
Metric 度量值	tos:0;k1 和 k3:1;k2,k4 和 k5:0

（续表）

特　　性	默认设置
网络	未指定
NSF Awareness	启用
偏移量	禁用
路由器 EIGRP	禁用
Metric 设置	未设置
通信共享	分配
变量	1

12.11.2 配置基本 EIGRP 参数

在特权 Exec 模式下开始，配置 EIGRP。

① 进入全局配置模式。

```
Router # configure terminal
```

② 启用一个 EIGRP 路由进程，并进入路由配置模式。

```
Router (config-router) # router eigrp autonomous-system
```

③ 将 EIGRP 路由关联到指定的网络。

```
Router (config) # network network-number
```

④（可选）启用 EIGRP 相邻改变日志，监视路由系统的稳定性。

```
Router (config) # eigrp log-neighbor-changes
```

⑤（可选）调整 EIGRP Metric。大多数情况下，采用默认值就可以很好地工作，因此通常无需修改。

```
Router (config) # metric weights tos k1 k2 k3 k4 k5
```

⑥ 将偏移列表应用到路由 Metric。可以借助访问列表或接口限制偏移列表。

```
Router (config) # offset list [access-list number | name] {in | out} offset
[type number]
```

⑦（可选）关闭自动归纳功能。EIGRP 自动在有类别网络边界归纳路由。但是在某些情况下，可能希望判断这一功能，比如当有不连续子网时。EIGRP 路由器在它不参与的网络中不进行自动网络归纳。

```
Router (config) # no auto-summary
```

⑧（可选）配置归纳路由。

```
Router (config) # ip summary-address eigrp autonomous-system-number address
mask
```

⑨ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑩ 校验配置。

```
Router # show ip protocols
```

⑪ 保存配置。

```
Router # copy running-config startup-config
```

使用这些命令的“no”形式来禁用这些特性或返回默认配置。

12.11.3 配置 EIGRP 接口

在特权 Exec 模式下开始，借助以下操作，可以配置 EIGRP 接口。

① 进入全局配置模式。

```
Router # configure terminal
```

② 进入接口配置模式，并指定欲配置的三层接口。

```
Router (config) # interface interface-id
```

③（可选）配置接口上 EIGRP 占用的带宽百分比。

```
Router (config) # ip bandwidth-percent eigrp percent
```

④（可选）为指定接口配置归纳地址。

```
Router (config) # ip summary-address eigrp autonomous-system-number address mask
```

⑤（可选）修改 EIGRP 路由进程的 hello 时间间隔。

```
Router (config) # ip hello-interval eigrp autonomous-system-number seconds
```

⑥（可选）修改 EIGRP 路由进程的 hold 时间间隔。

```
Router (config) # ip hold-time eigrp autonomous-system-number seconds
```

⑦（可选）禁用水平分割，允许路由接口被路由器公布。

```
Router (config) # no ip split-horizon eigrp autonomous-system-number
```

⑧ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑨ 校验配置。

```
Router # show ip eigrp interface
```

⑩ 保存配置。

```
Router # copy running-config startup-config
```

使用这些命令的“no”形式禁用这些特性或返回默认配置。

12.11.4 配置 EIGRP 路由认证

从特权 Exec 模式下开始，借助以下操作，启用 EIGRP 路由认证。

① 进入全局配置模式。

```
Router # configure terminal
```

② 进入接口配置模式，并指定欲配置的三层接口。

```
Router (config) # interface interface-id
```

③ 在 IP EIGRP 包内启用 MD5 认证。

```
Router (config) # ip authentication mode eigrp autonomous-system md5
```

④ 启用 IP EIGRP 包的认证。

```
Router (config) # ip authentication key-chain eigrp autonomous-system key-chain
```

⑤ 返回全局配置模式。

```
Router (config-if) # exit
```

⑥ 标识密钥链并进入 key-chain 配置模式。

```
Router (config) # key chain name-of-chain
```

⑦ 在 key-chain 配置模式中，标明密钥号。

```
Router (config) # key number
```

⑧ 在 key-chain 配置模式中，指定密钥字符串。

```
Router (config) # key-string text
```

⑨（可选）指定密钥被接收的时间段。

```
Router (config) # accept-lifetime start-time {infinite | end-time | duration seconds}
```

⑩（可选）指定关键字被发送的时间期间。

```
Router (config) # send-lifetime start-time {infinite | end-time | duration seconds}
```

⑪ 返回特权 Exec 模式。

```
Router (config-if) # end
```

⑫ 显示认证关键信息。

```
Router # show key chain
```

⑬ 保存配置。

```
Router # copy running-config startup-config
```

使用这些命令的“no”形式来禁用这些特性或返回默认配置。

12.11.5 监控 EIGRP

从邻居表中删除相邻路由。

clear ip eigrp neighbors [*if-address* **|** *interface*]

显示 EIGRP 接口的信息。

show ip eigrp interface [*interface*] [*as number*]

显示 EIGRP 发现的邻居。

show ip eigrp neighbors [*type-number*]

显示 EIGRP 拓扑表。

show ip eigrp topology [*autonomous-system-number*] | [[*ip-address*] *mask*]

显示数据包发送和接收的数量。

show ip eigrp traffic [*autonomous-system-number*]

第 13 章　使用 CLI 管理路由器

路由器的管理方式和命令行与交换机基本相同。例如，软件映像的备份与恢复，配置文件的备份与恢复，甚至包括文件和文件夹的管理，等等。因此，在这里只介绍与交换机管理不同的内容。

13.1　CF 内存卡的管理

Cisco 3900/2900/1900 系列集成服务路由器（Integrated Services Routers，ISR）使用高性能 CF（Advanced Capability Compact Flash）卡扩充内存存储系统映像、配置文件和一些软件数据文件。CF 支持 True IDE 模式和 Multi-Word DMA 模式。

13.1.1 需求和限制

1.　CF 卡支持

Cisco 3900/2900/1900 系列路由器只支持专用的 CF 卡。如果在路由器中插入非专用 CF 卡，将显示如下错误提示消息：

WARNING: Unsupported compact flash detected. Use of this card during normal operation
can impact and severely degrade performance of the system. Please use supported
compact flash cards only.

2.　格式化 CF 卡

Cisco CF 卡只支持 C 类文件系统。

推荐格式化 CF，以初始化为一个新的 Flash 文件系统。恰当地格式化，可以让 ROM 监控器识别并引导该 Flash 内存。CF 卡既可以在 ISR 路由器中格式化，也可以在安装有 CF 读卡器的计算机上格式化并备份文件。如果使用计算机格式化 CF 卡，应当使用 FAT32（Microsoft File Allocation Table）文件系统。

3.　CF 插槽和文件

Cisco 3900/2900/1900 系列路由器拥有 2 个扩展 CF 插槽。位于 Slot0 插槽中的 CF 卡可以存储系统映像、配置文件和数据文件。在路由器引导和执行文件操作时，CF 卡必须位于 CF 插槽中。CF 插槽编号和文件名、大小如表 13-1 所示。

Cisco 3800/2800/1800 系列路由器则只拥有 1 个扩展 CF 插槽。所以，无需特别指定使用哪个 Flash 插槽。

表 13-1 Cisco 3900/2900/1900 系列 CF 插槽编号和文件名、大小

插槽编号	CF 文件名	大 小
Slot0	flash0:	256 MB
Slot1	flash1:	0

注：Slot0 和 Slot1 插槽中的 CF 卡最大容量为 4 GB。Slot0 默认 CF 插槽。

4. CF 卡的插拔

路由器允许在正常运行时插拔 CF 卡，即支持在线插拔（Online insertion and removal，OIR）和更换，而无需关闭路由器，不会影响其他接口的正常运行。CF 卡的 OIR 特性，保证了在设备维护时网络的不间断运行。

需要特别注意的是，尽管路由器支持 OIR，但是，绝对不能在 CF 插槽的 LED 指示灯闪烁时进行插拔。LED 灯闪烁表明有软件正在访问 CF 内存卡，此时移除 CF 内存卡，很有可能将导致网络的中断，因为软件需要使用 CF 卡存储表格或其他重要数据。

13.1.2 格式化 CF 卡

1. 确定 CF 内存卡的文件系统

若欲确定 CF 内存卡的文件系统，可以在特权 Exec 模式下使用 show flash: all 命令。在语法中使用 flash1:，显示插槽 1 中的 CF 卡；使用 flash0:，显示插槽 0 中的 CF 卡。

如果输出信息中没有显示 Geometry 和 Format 信息，表示该 CF 卡以 B 类 Flash 文件系统格式化。Cisco 3900/2900/1900 系列和 Cisco 3800/2800/1800 系列路由器不支持 B 类文件系统。

如果输出信息中显示有 Geometry 和 Format 信息，表示该 CF 卡以 C 类 Flash 文件系统格式化。

如下输出示例中，没有显示 Geometry 和 Format 信息，表明为 B 类文件系统。

```
Router# show flash: all
Partition Size Used Free Bank-Size State Copy
Mode
1 125184K 20390K 104793K 0K Read/Write
Direct
System Compact Flash directory:
File Length Name/status
addr fcksum ccksum
1 6658376 c29xx-i-mz
0x40 0xE0FF 0xE0FF
2 14221136 c2900-telcoent-mz
0x6599C8 0x5C3D 0x5C3D
[20879640 bytes used, 107308776 available, 128188416 total]
125184K bytes of ATA System Compact Flash (Read/Write)
Chip information NOT available.
```

如下输出示例中，显示有 Geometry 和 Format 信息，表明为 C 类 Flash 文件系统。

```
Router# show flash: all
-#- --length-- -----date/time------ path
1 6658376 Mar 01 2004 04:27:46 c28xx-i-mz
25268224 bytes available (6664192 bytes used)
******** ATA Flash Card Geometry/Format Info ********
ATA CARD GEOMETRY
Number of Heads: 4
Number of Cylinders 490
Sectors per Cylinder 32
Sector Size 512
Total Sectors 62720
ATA CARD FORMAT
Number of FAT Sectors 31
Sectors Per Cluster 8
Number of Clusters 7796
Number of Data Sectors 62560
Base Root Sector 155
Base FAT Sector 93
Base Data Sector 187
```

2. 将 CF 卡格式化为 C 类文件系统

在特权 Exec 模式下，使用 format flash0:命令，可以将 CF 卡格式化为 C 类 Flash 文件系统，或者移除 CF 内存卡中原有的文件。

例如，若欲格式化插槽 0 中的 CF 卡，则执行下述命令。

```
Router# format flash0:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash0:". Continue? [confirm]
Enter volume ID (up to 64 chars)[default flash]:
Current Low End File System flash card in flash will be formatted into DOS
File System flash card! Continue? [confirm]
Format:Drive communication & 1st Sector Write OK...
Writing Monlib sectors .............................................
Monlib write complete
Format:All system sectors written. OK...
Format:Total sectors in formatted partition:250592
Format:Total bytes in formatted partition:128303104
Format:Operation completed successfully.
Format of flash complete
```

13.1.3 CF 卡的文件操作

1. 复制文件

在特权 Exec 模式下使用 copy 命令，可以实现文件的复制操作。使用 flash1:或 flash0:，用于指定存储在插槽 1 或插槽 0 中 CF 卡上的文件。

例如，将插槽 0 中 CF 卡上的 my-config 文件复制至系统内存中的 startup-config 文件，命

令如下：

```
Router# copy flash0:my-config startup-config
Destination filename [startup-config]?
[OK]
517 bytes copied in 4.188 secs (129 bytes/sec)
```

2. 列出文件

若欲显示 CF 卡中的文件列表，在特权 Exec 模式下使用 dir flash0:命令。

例如，若欲列出插槽 0 中的 CF 卡上的文件，则执行下述命令。

```
Router# dir flash0:
Directory of flash0:/
1580 -rw- 6462268 Mar 06 2004 06:14:02 c2900-universalk9-mz.data
3 -rw- 6458388 Mar 01 2004 00:01:24 c2900-universalk9-mz.bin
63930368 bytes total (51007488 bytes free)
```

3. 显示文件内容

若欲查看 CF 卡中指定文件的内容，在特权 Exec 模式下使用 more flash0:命令。

例如，若欲查看插槽 0 中的 CF 卡上 c29xx-i-mz 文件的内容，则执行下述命令。

```
Router# more flash0:c29xx-i-mz
00000000: 7F454C46 01020100 00000000 00000000 .ELF .... .... ....
00000010: 00020061 00000001 80008000 00000034 ...a .... .... ...4
00000020: 00000054 20000001 00340020 00010028 ...T ... .4. ...(
00000030: 00050008 00000001 0000011C 80008000 .... .... .... ....
00000040: 80008000 00628A44 00650EEC 00000007 .... .b.D .e.l ....
00000050: 0000011C 0000001B 00000001 00000006 .... .... .... ....
00000060: 80008000 0000011C 00004000 00000000 .... .... ..@. ....
00000070: 00000000 00000008 00000000 00000021 .... .... .... ...!
00000080: 00000001 00000002 8000C000 0000411C .... .... ..@. ..A.
00000090: 00000700 00000000 00000000 00000004 .... .... .... ....
000000A0: 00000000 00000029 00000001 00000003 .... ...) .... ....
000000B0: 8000C700 0000481C 00000380 00000000 ..G. ..H. .... ....
000000C0: 00000000 00000004 00000000 0000002F .... .... .... .../
000000D0: 00000001 10000003 8000CA80 00004B9C .... .... ..J. ..K.
000000E0: 00000020 00000000 00000000 00000008 ... .... .... ....
000000F0: 00000000 0000002F 00000001 10000003 .... .../ .... ....
00000100: 8000CAA0 00004BBC 00623FA4 00000000 ..J ..K< .b?$ ....
00000110: 00000000 00000008 00000000 3C1C8001 .... .... .... <...
00000120: 679C4A80 3C018001 AC3DC70C 3C018001 g.J. <... ,=G. <...
00000130: AC3FC710 3C018001 AC24C714 3C018001 ,?G. <... ,$G. <...
00000140: AC25C718 3C018001 AC26C71C 3C018001 ,%G. <... ,&G. <...
00000150: AC27C720 3C018001 AC30C724 3C018001 ,'G <... ,0G$ <...
00000160: AC31C728 3C018001 AC32C72C 3C018001 ,1G( <... ,2G, <...
--More-- q
```

4. 显示 Geometry 和 Format 信息

若欲查看 CF 卡文件系统中的 Geometry 和 Format 信息，在特权 Exec 模式下使用 show flash0: filesys 命令。

例如，若欲查看插槽 0 中的 CF 卡上的 Geometry 和 Format 信息，则执行下述命令。

```
Router# show flash0: filesys
******** ATA Flash Card Geometry/Format Info ********
ATA CARD GEOMETRY
Number of Heads: 4
Number of Cylinders 490
Sectors per Cylinder 32
Sector Size 512
Total Sectors 62720
ATA CARD FORMAT
Number of FAT Sectors 31
Sectors Per Cluster 8
Number of Clusters 7796
Number of Data Sectors 62560
Base Root Sector 155
Base FAT Sector 93
Base Data Sector 187
```

5. 删除文件

在特权 Exec 模式下使用 delete flash0:命令，可以从 CF 卡中删除指定的文件。

例如，若欲删除插槽 0 中 CF 卡上的 my-config 文件，命令如下。

```
Router# delete flash0:my-config
```

6. 文件重命名

在特权 Exec 模式下使用 rename 命令，可以重命名 CF 卡中指定的文件。

例如，若欲将插槽 0 中 CF 卡上的 c2900-universalk9-mz.tmp 文件重命名为 c2900-universalk9-mz，执行下述操作。

```
Router# dir flash0:
Directory of flash0:/
3 -rw- 6458388 Mar 01 2004 00:00:58 c2900-universalk9-mz.tmp
1580 -rw- 6462268 Mar 06 2004 06:14:02 c2900-universalk9-mz.3600ata
63930368 bytes total (51007488 bytes free)
Router# rename flash0:c2900-universalk9-mz.tmp flash0:c2900-universalk9-mz
Destination filename [c2900-universalk9-mz]?
Router# dir flash0:
Directory of flash0:/
1580 -rw- 6462268 Mar 06 2004 06:14:02 c2900-universalk9-mz.3600ata
3 -rw- 6458388 Mar 01 2004 00:01:24 c2900-universalk9-mz
63930368 bytes total (51007488 bytes free)
```

13.1.4 CF卡的目录操作

1. 进入目录

在特权Exec模式下使用cd命令，可以进入CF卡中指定的目录。cd命令用于指定或改变默认的目录或文件系统。如果只键入 cd 命令，而不指定文件系统，路由器将进入默认 home 目录，即flash0。如果键入cd flash1:，则路由器进入flash1目录。

例如，若欲进入home目录，则键入如下命令。

```
Router# cd
```

在特权Exec模式下使用dir命令，可以显示当前进入目录中的文件和文件系统。

```
Router# dir
Directory of flash0:/
1580 -rw- 6462268 Mar 06 2004 06:14:02 c2900-universalk9-mz.3600ata
3 -rw- 6458388 Mar 01 2004 00:01:24 c2900-universalk9-mz
63930368 bytes total (51007488 bytes free)
```

若欲进入config目录，则键入如下命令。

```
Router# cd config
```

在特权Exec模式下使用pwd命令，可以确定目前进入的是哪个目录。

```
Router# pwd
flash0:/config/
Router# dir
Directory of flash0:/config/
380 -rw- 6462268 Mar 08 2004 06:14:02 myconfig1
203 -rw- 6458388 Mar 03 2004 00:01:24 myconfig2
63930368 bytes total (51007488 bytes free)
```

2. 创建新目录

在特权Exec模式下使用mkdir flash0:命令，可以创建新目录。

例如，若欲在flash0的config目录中创建test-config子目录，执行下述操作。

```
Router# dir flash0:
Directory of flash0:/
1580 -rw- 6462268 Mar 06 2004 06:14:02 c2900-universalk9-mz.3600ata
3 -rw- 6458388 Mar 01 2004 00:01:24 c2900-universalk9-mz
63930368 bytes total (51007488 bytes free)
Router# mkdir flash0:/config
Create directory filename [config]?
Created dir flash0:/config
Router# mkdir flash0:/config/test-config
Create directory filename [/config/test-config]?
Created dir flash0:/config/test-config
```

```
Router# dir flash0:
Directory of flash0:/
3 -rw- 6458208 Mar 01 2004 00:04:08 c2900-universalk9-mz.tmp
1580 drw- 0 Mar 01 2004 23:48:36 config
128094208 bytes total (121626624 bytes free)
```

3. 移除目录

在特权 Exec 模式下使用 rmdir flash0:命令，可以移除已经存在的目录。不过，在移除某个目录之前，必须移除其中所有的子目录和文件。

例如，若欲移除 flash0 中 config 目录下的 test-config 子目录，执行如下操作。

```
Router# dir
Directory of flash0:/config/
1581 drw- 0 Mar 01 2004 23:50:08 test-config
128094208 bytes total (121626624 bytes free)
Router# rmdir flash0:/config/test-config
Remove directory filename [/config/test-config]?
Delete flash0:/config/test-config? [confirm]
Removed dir flash0:/config/test-config
Router# dir
Directory of flash0:/config/
No files in directory
128094208 bytes total (121630720 bytes free)
```

13.2 系统映像和配置文件的管理

13.2.1 选择 Cisco IOS 软件版本

选择 Cisco IOS 软件版本应当主要考虑以下几个方面因素。

- 硬件支持。
- 功能支持。
- Cisco IOS 软件发行版本。
- 内存需求。

1. 硬件支持

首先检查选择的 Cisco IOS 软件发行版本是否被硬件所支持。可以在随设备附送的文档 CD 中的 Cisco 产品文档（Cisco Product Documentation）部分找到该硬件设备所需的软件。不过，Cisco 推荐使用“Cisco 软件顾问”（Cisco Software Advisor）来搜索 Cisco IOS 支持的硬件。

为了更好地选择软件版本，需要做好以下工作。

- 搜集支持所有硬件设备不同软件版本列表。
- 确定在网络中需要部署的功能。

有关功能、硬件支持和其他特殊 IOS 版本，应当参考 Cisco 网站（http://www.cisco.com）

的“Cisco IOS Software”页面。

2. 功能支持

在 Cisco 设备使用 show version 命令显示输出版本信息，使用 Output Interpreter Tool（需要用户注册）显示潜在的故障和补丁包。

检查软件所支持的功能是非常重要的步骤，特别是需要在网络中部署该功能时。如果想保持目前路由设备中运行软件的相同功能，但是不能确定哪些功能设置是自己所需要的，可以在路由器上执行 show version 命令。

为了寻找能够支持计划部署的所有功能的 Cisco IOS 软件，建议访问 Cisco 功能导航页面（http://www.cisco.com/go/cfn），或者使用 Cisco Software Advisor，根据功能或版本进行搜索，甚至可以允许比较两个不同的版本。写下所有能够满足需要的不同软件版本，然后，再与硬件兼容性比较核对。

3. 软件发行版本

Cisco IOS 软件命名的格式类似于 A.B(C)D。

- B 和 C 是数字。
- D（如果出现）是字母。
- B 是主要发行版本。
- C 是维护版本。较高的维护数字意味着更多的补丁修复。
- D（如果出现）表明是一个非主要版本，是对主要版本的扩展。这些扩展通常提供新的特性和新的硬件支持。

> **提·示** 旧版本往往比新版本更稳定，但功能也更少。

The Cisco IOS 软件映像是 ED、LD、GD 和 DF 之一。

ED（Early Deployment，早期部署）版本。ED 版本往往提供较多的新功能、平台和接口支持。多数主要版本都包括 ED 版本。

GD（General Deployment，普遍部署）版本。如果 Cisco 认为 Cisco IOS 软件的主要版本适合在客户网络中需要这些特性和功能的任何地方使用，则这种主要版本进入“普遍部署”阶段。进入“普遍部署”阶段的标准主要是客户反馈调查、客户工程师故障报表，以及报告的现场实际运行情况。只有主要版本才能进入普遍部署阶段。

LD（Limited Deployment，有限部署）版本。LD 版本介于初次发售到进入 GD 阶段之间，Cisco IOS 软件的主要版本处于其生命周期的“有限部署”阶段。

DF（Deferred，延期）版本。因为存在众所周知的缺陷，DF 版本不可以下载。在路由器上也不要安装这些版本。

在选择版本时，建议尽量采用 GD 版本。只有在硬件和软件特性无法作出其他选择时，才采用 ED 版本。

4. 内存需求

在向路由器安装新的 Cisco IOS 软件映像之前，检查路由器能够提供软件映像所需的空间。使用 show version，可以查看内存容量。

```
...
cisco RSP4 (R5000) processor with 65536K/2072K bytes of memory
...
16384K bytes of processor board System flash (Read ONLY)
```

第一行显示路由器中有多少动态内存（Dynamic RAM，DRAM）和封装内存（Packet memory）。有些平台将一部分 DRAM 划分出来作为 Packet 内存，那么，路由器上所有 DRAM 的总和就是可用内存。

示例 1：DRAM 和 Packet 内存是单独的。

```
...
cisco RSP4 (R5000) processor with 65536K/2072K bytes of memory
...
```

Cisco 4000/4500/4700/7500 路由器有单独的 DRAM 和 Packet 内存，只需查看第一个数字，此处显示路由器拥有 65 536 KB（或 64 MB）DRAM。

示例 2：DRAM 和 Packet 内存是组合的。

```
...
cisco 2611 (MPC860) processor (revision 0x202) with 29696K/3072K bytes of memory
...
```

Cisco 1000/1600/2500/2600/3600/7200 路由器使用部分 DRAM 作为 Packet 内存，需要将找到的内存数值相加才是真正的 DRAM 总量。例如，路由器拥有 2 969 KB + 3 072 KB = 32 768 KB（或 32 MB）DRAM.

示例 3：可用 Flash 内存。

```
...
cisco RSP4 (R5000) processor with 65536K/2072K bytes of memory
...
```

16384K bytes of processor board System flash (Read ONLY)

下面一行显示有多少 Flash 内存可用，因为有些 Flash 可能已经被使用。若欲查看空闲 Flash 内存总量，执行 show flash 命令。

```
Router#show flash

System flash directory:
File   Length   Name/status
  1    8407884  c2600-io3s56i-mz.121-6
[8407948 bytes used, 8369268 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

5. 映像下载

如果想了解自己欲下载的 Cisco IOS 版本和功能设置，可以直接访问以下 URL：

http://www.cisco.com/kobayashi/sw-center/index.shtml.

若欲获得更多关于 Cisco IOS 版本和功能设置的信息，可以直接访问软件下载中心：

http://www.cisco.com/public/sw-center/index.shtml.

更多有关软件映像下载和管理的信息，请访问如下 URL：

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_system_images.html

13.2.2 更新路由器系统映像

更新系统映像主要操作步骤如下。

① 备份原有的系统映像和配置文件。

② 确保新的系统映像有足够的 DRAM 内存。

③ 确保新的系统映像有足够的 Flash 内存。

④ 将系统映像复制至 Flash 内存。

⑤ 装载新的系统映像。

⑥ 备份新的系统映像和配置文件。

1. 备份旧的系统映像和配置

由于升级系统后，现有的配置文件将会丢失，因此，必须备份现有的配置文件（既可以备份 running-config 也可以备份 startup-config）。另外，为了保证在系统映像升级失败后，能够恢复原来的系统映像，自然也需要备份现有的系统映像。

① 进入全局配置模式。

```
Router> enable
```

② 将 running-config 或 startup-config 备份至 FTP、RCP 或 TFTP 服务器。在系统提示时，键入服务器的 URL。

```
Router# copy nvram:startup-config {ftp: | rcp: | tftp:}
Router# copy running-config {ftp: | rcp: | tftp:}
```

> **提·示** 执行该操作前，应当确认相应的 FTP、RCP 或 TFTP 服务器已经运行，并能够提供正常服务。

③ 列出 Flash 闪存中的系统映像的文件名称。

```
Router# dir flash:
```

④ 将闪存中原有的系统映像文件复制至 FTP、RCP 或 TFTP 服务器。在系统提示时，键入闪存的分区号，以及文件名和目的 URL。

```
Router# copy flash: {ftp: | rcp: | tftp:}
```

示例：

将 Startup Configuration 和系统映像备份至 TFTP 服务器。TFTP 服务器的 IP 地址为 192.168.0.1，Cisco 2800 原有系统映像的文件名为 c2800-image-mz。

```
Router# copy nvram:startup-config tftp:
Remote host[]? 192.168.0.1
Name of configuration file to write [r2-confg]? r2-config-upgrade
Write file rtr2-confg-b4upgrade on host 192.168.0.1?[confirm] <回车>
![OK]
Router# dir flash:
System flash directory:
File Length Name/status
1 4137888 c2800-image-mz
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\
Router# copy flash: tftp:
IP address of remote host [255.255.255.255]? 192.168.0.1
filename to write on tftp host? c2800-image-mz
writing c2800-image-mz !!!!...
successful ftp write.
```

2. 确认系统映像有足够可用的内存

下载新的 Cisco IOS 系统映像，在 Cisco 官方网站（http://www.cisco.com/cisco/software/navigator.html）查阅并记录该系统映像所需的 DRAM 内存和 Flash 闪存容量。

使用 show version 命令，查看并计算 DRAM 内存大小，并确认是否能够满足新版本系统映像的最小需求。如果 DRAM 大于系统映像的最小需求，可以继续执行映像文件的升级；如果 DRAM 小于系统映像的最小需求，则必须增加或更换 DRAM 内存条。

示例：

```
Router# show version
Cisco IOS Software, 2800 Software (C2800NM-SPSERVICESK9-M), Version 12.4(9)T7, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jan-08 16:35 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
…
Cisco 2821 (revision 53.51) with 251904K/10240K bytes of memory.
Processor board ID FHK1210F28A
2 Gigabit Ethernet interfaces
4 Voice FXO interfaces
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
125440K bytes of ATA CompactFlash (Read/Write)
```

```
Configuration register is 0x2102
```

其中，DRAM 内存大小为 251 904 KB+10 240 KB=262 144 KB，即 256 MB。

3. 确认系统映像有足够可用的 Flash 闪存

① 收回先前删除文件所占用的磁盘空间。

```
Router# squeeze flash:
```

② 查看 Flash 闪存中可用的（available）和总的（total）容量大小。如果可用容量大于新的系统映像文件的最小需求，可以直接将其复制至 Flash 闪存。如果可用容量且总容量均小于新的系统映像文件的最小需求，需要更换容量更大的 Flash 闪存卡。如果总容量能够满足新映像的最小需求，但是，可用容量不能满足时，可以考虑备份并删除现有的系统映像。

```
Router# dir flash:
```

③ 显示 Flash 闪存中所有文件和目录列表，记录删除系统映像或配置文件的名称。

```
Router# dir /all flash:
```

④ 将欲删除的系统映像或配置文件备份至 TFTP 或 RCP 服务器。重复操作，直至将所有欲删除的文件都备份至服务器。

```
Router# copy flash: {tftp | rcp}
```

⑤ 删除不再需要的文件。重复操作，直至删除所有不再需要的文件。

```
Router# delete flash:directory-path/filename
```

⑥ 收回刚刚删除文件所占用的磁盘空间。

```
Router# squeeze flash:
```

⑦ 再次查看 Flash 闪存可用空间是否能够满足新映像文件的需要。

```
Router# dir flash:[partition-number:]
```

示例：

```
Router# squeeze flash:
Squeeze operation may take a while. Continue? [confirm]
squeeze in progress...
sssssssssssssssssssssssssseeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Rebuild file system directory...
Squeeze complete
Router# dir flash:
Flash CompactFlash directory:
File Length Name/status
1 6458208 c38xx-i-mz.tmp [deleted]
2 6458208 c38xx-i-mz
```

```
[12916544 bytes used, 3139776 available, 16056320 total]
15680K bytes of ATA CompactFlash (Read/Write)
Router# dir /all flash:
Directory of flash:/
3 -rw- 6458388 Mar 01 1993 00:00:58 c38xx-i-mz.tmp
1580 -rw- 6462268 Mar 06 1993 06:14:02 c38xx-i-mz.2800ata
63930368 bytes total (51007488 bytes free)
Router# copy flash tftp
Router# delete flash:c38xx-i-mz.tmp
Delete filename [c38xx-i-mz.tmp]? <回车>
Delete flash:c38xx-i-mz.tmp? [confirm] <回车>
Router# squeeze flash:
Squeeze operation may take a while. Continue? [confirm]
squeeze in progress...
sssssssssssssssssssssssseeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Rebuild file system directory...
Squeeze complete
Router# dir flash:
Flash CompactFlash directory:
File Length Name/status
1 6458208 c38xx-i-mz.tmp [deleted]
2 6458208 c38xx-i-mz
[12916544 bytes used, 3139776 available, 16056320 total]
15680K bytes of ATA CompactFlash (Read/Write)
```

4. 将新的系统映像复制至 Flash 闪存

■ **使用 TFTP 或 RCP 服务器复制**

① 从 TFTP 或 RCP 服务器将系统映像复制至路由器 Flash 闪存。

```
Router# copy tftp flash
```

或

```
Router# copy rcp flash
```

> **提示** 执行该操作前，应当确认相应的 TFTP 或 RCP 服务器已经运行，并能够提供正常服务。同时，确认已经将新的系统映像下载并复制至服务器指定的默认文件夹中。

② 键入 TFTP 或 RCP 服务器的 IP 地址。

```
Address or name of remote host []? 192.168.0.1
```

③ 键入欲安装的 Cisco IOS 软件映像的文件名。

```
Source filename []? c2800-i-mz.124-14.bin
```

提·示　Cisco IOS 软件映像文件名区分大小写。

④ 键入欲应用至路由器的 Cisco IOS 软件映像名称。

```
Destination filename []? c2800-i-mz.124-14.bin
```

⑤ 如果系统提示“Not enough space on device”（没有足够的空间），根据情况执行下述两者之一。

- 如果确认 Flash 闪存中所有的文件都可以被删除，键入两次“y”，则闪存中所有的文件都将被删除。
- 如果不能确认所有的文件都可以被删除，则键入 Ctrl+Z 组合键中止当前操作，手工删除不再需要的文件以释放空间。

```
Accessing tftp://192.168.0.1/ c2800-i-mz.124-14.bin...
Erase flash: before copying? [confirm] y
Erasing the flash filesystem will remove all files! Continue? [confirm] y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
```

⑥ 如果没有显示错误信息，则键入“no”，这样，在向 Flash 闪存中复制文件时，将不会删除其中的文件。

```
Accessing tftp://192.168.0.1/ c2800-i-mz.124-14.bin...
Erase flash: before copying? [confirm] no
```

■ **使用计算机复制**

由于系统文件存在外部 CF 内存卡中，因此，可以使用计算机和 CF 卡的读卡器格式化 CF 卡，并且将新的系统文件复制至 CF 卡。

13.2.3 将路由器恢复至出厂默认设置

如果需要重新配置路由器，或者将路由器移动到其他位置时，都需要将路由器恢复至出厂默认值，以避免配置时可能出现的错误。

1. 方法一

该方法在全局模式下使用 config-register 0x2102 命令实现。

① 在路由器上使用 show version 命令，检查寄存器配置。

```
Router# show version
```

② 进入全局配置模式。

```
Router# configure terminal
router(config)#
```

③ 将寄存器值修改为 0x2102。再次使用 show version 命令查看寄存器值，将显示“will be 0x2102 at next reload”，即下将重新装载系统后，寄存器值将修改为 0x2102。

```
router(config)#config-register 0x2102
```

④ 使用 write erase 命令，删除路由器上当前的启动配置。

```
Router(config)# write erase
```

⑤ 返回至特权 EXEC 模式。

```
router(config)#end
```

⑥ 重新引导路由器，并在系统提示是否保存配置时，输入“n”。

```
router#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
```

⑦ 在路由器引导完成后，将显示系统配置对话程序。至此，路由器已经恢复至原始出厂默认设置。

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

2. 方法二

该方法在全局模式下使用 config-register 0x2142 命令实现。

① 在路由器上使用 show version 命令，检查寄存器配置。

```
Router# show version
```

② 进入全局配置模式。

```
Router# configure terminal
router(config)#
```

③ 将寄存器值修改为 0x2142。再次使用 show version 命令查看寄存器值，将显示“will be 0x2142 at next reload”，即下将重新装载系统后，寄存器值将修改为 0x2142。

```
router(config)#config-register 0x2142
```

④ 返回至特权 EXEC 模式。

```
router(config)#end
```

⑤ 重新引导路由器，并在系统提示是否保存配置时，输入“n”。

```
router#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
```

⑥ 在路由器引导完成后，将显示系统配置对话程序，在“Would you like to enter initial

configuration dialog?”提问中输入“no”。

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:no
```

⑦ 重新引导完成后，再次进入全局配置模式，并将寄存器值修改为 0x2102。

```
Router# configure terminal
router(config)#config-register 0x2102
```

⑧ 返回至特权 EXEC 模式，使用 write memory 命令，以当前的运行配置覆盖原来的启动配置。

```
Router(config)# end
router# write memory
```

⑨ 使用 reload 命令，重新启动路由器。路由器成功启动后，显示系统配置对话程序。至此，路由器已经恢复至出厂默认值。

```
router#reload
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

第 14 章　安全设备概述

近年来，网络所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险，如黑客攻击、蠕虫病毒、木马后门、间谍软件、僵尸网络、DDoS 攻击、垃圾邮件、网络资源滥用（P2P 下载、IM 即时通信、网游、在线视频）等，极大地困扰着用户，给企业的信息网络造成严重的破坏。能否及时发现并成功阻止网络黑客的入侵，保证计算机和网络系统的安全和正常运行，便成为所有网络都必须面对的一个重要问题。

14.1　网络防火墙

防火墙的英文名称为“Fire Wall”，是目前最重要的一种网络防护功能。网络防火墙的主要功能就是抵御外来非法用户的入侵，就像是矗立在内部网络用户和外部网络之间的一道安全屏障，外部网络用户的访问必须先经过安全策略过滤，而内部网络用户对外部网络的访问，则无需过滤。而这些过滤策略就是防火墙工作的主要依据。另外，网络防火墙还具有隔离网段、提供代理服务、流量控制等功能，可以满足用户的各种需求。

14.1.1　网络安全防护的重要意义

无论是大中型企业网络，还是小型家庭办公网络，对网络安全方面的要求一直保持上升趋势。微软公司的官方网站尚且难逃黑客的魔爪，普通的中小网络更是难以抵抗了。解决网络安全问题最常用的防护手段就是安装网络防火墙，对于大中型规模的企业网络而言尤其如此。

无论是黑客有意的攻击，还是用户无意的误操作，都可能会给系统带来不可估量的损失。攻击者可以窃听网络上的信息，窃得用户的密码，窃取数据库的信息；还可以篡改数据库内容，伪造用户身份，伪造自己的签名。更有甚者，攻击者可以删除数据库内容，摧毁网络节点，释放计算机病毒，等等。

事实上，企业面对的信息安全问题正在变得复杂化。从便携设备到可移动存储，再到基于 Web 的协作应用，乃至基于 IP 的语音技术（VoIP），每一类新产品都有新的安全问题与之相伴而生。系统在面临着日趋复杂的威胁的同时，遭受攻击的次数也日益增多。对此，安全专家和业务技术人员列出了企业所面临的一长串挑战，按比例依次为：提高用户意识（41%）、加强安全策略（36%）、加强对系统访问的控制（26%），以及获取更多的资源（23%）。

超过半数的业务技术专家表示，当企业现有和以前的雇员企图危及系统安全时，安全技术、政策和培训在阻止其制造安全漏洞方面几乎起不到什么作用。

去年，将近四分之一的美国公司表示，授权用户和雇员是引起攻击的原因之一，印度公司、中国公司和欧洲公司的相应比例分别为 22%、15%和 11%。内部工作人员能较多地接触内

部信息，工作中的任何不小心都可能给信息安全带来危险。这些都使信息安全问题越来越复杂。几乎可以肯定地说，任何形式的 Internet 服务都可能存在安全方面的风险，即便是收发电子邮件和信息共享也不例外。

目前，大多数网络安全解决方案提供的只是“网络安全风险管理”。所谓“网络安全风险管理”，就是对网络本身存在的脆弱性和针对网络的威胁进行最小化。最佳的解决方案是不断改善预防性措施，选择最能适合自身实际的网络安全解决方案。一个网络通常面临着三类脆弱性：行为管理脆弱性、网络配置脆弱性和技术脆弱性。

当人们不知道什么可以做或者什么不可以做时，“行为管理”问题就凸现出来了。例如，当公司的员工绕开公司的防火墙，在笔记本电脑上使用 3G 上网卡，通过当地的 ISP（Internet Service Provider，因特网服务提供商）连接 Internet 时，一个公司局域网内部的“后门”就暴露出来了。这就是一个公司的“网络安全行为管理”所不能容许的。“网络配置”问题也很容易发生。例如，当一个员工在配置防火墙，尤其是配置界面友好的图形界面（Graphical User Interface，GUI）类防火墙时，一旦有所闪失，就会产生“网络配置错误”。“技术脆弱性”是指操作系统的漏洞和缓冲溢出等。

事实上，没有任何一种技术可完全消除网络中的安全漏洞，网络安全实际上是理想中的安全策略和实际的执行之间的一个平衡。网络安全不仅仅是技术问题，更是一个管理问题，它包含管理机构、法律、技术、经济各方面，网络安全技术只是实现网络安全的工具，因此，一个优秀的企业网络必须要有一个综合的网络安全解决方案。

14.1.2 网络防火墙简介

“防火墙”的本意是指发生火灾时，用来防止火势蔓延的一道障碍物，一般都修筑在建筑物之间。而如今的网络防火墙则是指设置在计算机网络之间的一道隔离装置，可以隔离两个或者多个网络、限制网络互访，以保护网络用户的安全。

网络防火墙最初的设计思想是，对内部网络总是信任的，对外部网络总是不信任的，所以当初的防火墙只能对外部进入的通信数据进行过滤，而对内部网络用户发出的信息不做任何限制。目前，最新的分布式防火墙系统在过滤机制上有所改变，不仅对外部网络发送过来的数据进行过滤，对内部网络用户发出的部分连接请求和数据包同样需要过滤，但防火墙仍然只是让符合安全策略的数据包通过。

总之，网络防火墙就是计算机网络中，工作在两个或者多个网络之间的一种硬件设备，一般包括以下几个基本特性。

■ 网络之间的所有网络数据包都必须经过防火墙过滤

这是网络防火墙在网络中位置的特性，同时也是一个实现过滤功能的前提。因为只有当防火墙是网络之间数据传输的唯一通道时，才可能对所有的数据包进行筛选，以拒绝非法用户的入侵。

根据美国国家安全局制订的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即采用不同安全策略的两个网络的连接处，如用户和 Internet 之间、同一企业内部同部门的网络之间等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过设定一定的筛选机制来决定允许或拒绝数据包通过，实现对进入

网络内部的服务和访问的审计和控制。

一般的防火墙体系网络结构如图 14-1 所示，从图中可以看出网络防火墙是内、外网络数据传输的必经之路。

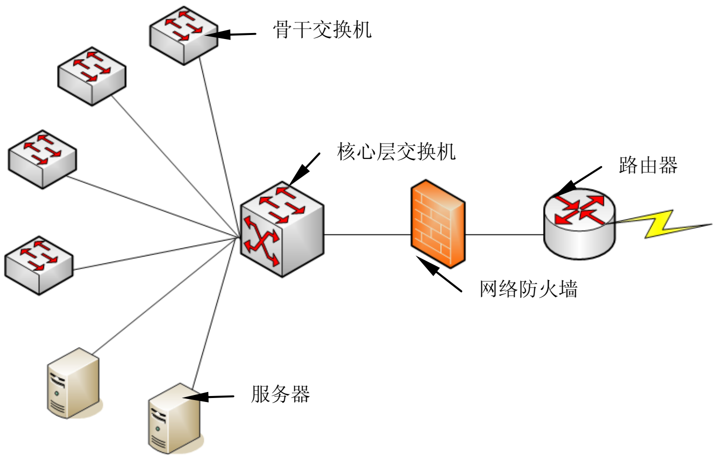


图 14-1 防火墙体系网络结构

■ **只有符合相应安全策略的数据包才可以通过防火墙**

这是网络防火墙工作原理的主要特性。防火墙之所以能够对内部网络起到一定的安全防护作用，主要依据的是网络管理员设置的数据包过滤机制。这些过滤机制使得允许通过的数据包不受任何影响，而不允许的数据包则全部拒绝在内部网络之外。如果没有这些过滤机制，防火墙将起不到任何安全防护作用。

■ **防火墙自身应具有非常强的抗攻击能力和免疫力**

这是防火墙之所以能够担当网络安全防护重任的先决条件。网络防火墙本来就处于网络的边缘，就像成边站岗放哨的战士一样，每时每刻都可能面对非法入侵的数据包，因此防火墙自身必须要具有非常强的抗入侵本领。它之所以具有如此强的本领，与其操作系统是分不开的，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。其次就是防火墙具有非常低的服务功能，除了专业的防火墙嵌入系统外，再没有其他应用程序在防火墙上运行，如图 14-1 所示。

14.1.3 防火墙的主要功能

防火墙的主要功能，一般来说主要有以下几个方面。

1. 创建一个阻塞点

防火墙在内部网络和外部网络之间建立一些检查点，这就要求所有的数据包都要通过这个检查点。一旦这些检查点清楚地建立，防火墙设备就可以监视并过滤和检查所有进来和出去的流量。网络安全产业称这些检查点为“阻塞点”。通过强制所有进出流量都通过这些检查点，网络管理员可以集中在较少的地方来实现安全目的。如果没有这样一些供监视和控制

信息的点，系统或安全管理员则要在大量的地方来进行监测。其实这些检查点也就是我们所说的网络边界。

2. 隔离不同的网络

防火墙最基本的功能就是隔离内、外网络，不仅确保不让非法用户入侵，更要保证内部信息的外泄。非法用户的入侵主要是通过获取对方的用户名和密码，以及其他一些重要的信息来实现的，甚至企业网络的内部数据更是黑客觊觎已久的肥肉，内部网络中不被人注意的一个细节可能包含了有关安全的线索，从而为攻击者留下可乘之机。使用防火墙则可以屏蔽这些内部细节，如 Finger、DNS 等服务。Finger 服务可以显示主机的所有用户的注册名和真名、最后登录时间和使用 shell 类型等，Finger 显示的信息非常容易被攻击者截获，攻击者通过所获取的信息可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网等信息。

3. 强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如密码、加密、身份证、审计等）设置在防火墙上。这比将网络安全分散到每个主机上，管理更集中而且更经济。各种安全措施的有机结合，更能有效地对网络安全性能起到加强作用。

4. 包过滤

包过滤是所有防火墙都具有的基本功能，由最初的 IP 地址、端口判定控制，到今天的判断通信报文协议头的各部分，以及通信协议的应用层命令、内容、用户认证、用户规则甚至状态检测，等等，无不标志着包过滤的进步。特别是状态监测技术，可以支持多种协议和应用程序，并可以很容易地实现应用层的扩充。它在现有协议栈中加载一个检测模块，模块在网络层截取数据包，然后在所有的通信层上抽取有关的状态信息，根据该状态位判断该通信是否符合安全策略。

5. 网络地址转换

网络地址转换（Network Address Translation，NAT）功能似乎已经成了防火墙的“隐身术”，绝大多数防火墙都加入了该功能。目前防火墙一般采用双向 NAT，即 SNAT（Stateless NAT）和 DNAT（Destination NAT）。SNAT 用于对内部网络地址进行转换，对外部网络隐藏起内部网络的结构，使得对内部的攻击更加困难；并可以节省 IP 资源，有利于降低成本。而 DNAT 主要用于实现外网主机对内网和 DMZ 区主机的访问。

6. 流量控制和统计分析

流量控制可以分为基于 IP 地址的控制和基于用户的控制。基于 IP 地址的控制是对通过防火墙各个网络接口的流量进行控制，基于用户的控制是通过用户登录来控制用户的流量，从而防止某些应用或用户占用过多的资源。而且通过流量控制可以保证重要用户和重要接口的连接。流量统计是建立在流量控制基础之上的。一般防火墙通过对基于 IP、服务、时间、协议等进行统计，可以与管理界面实现挂接，实时或者以统计报表的形式输出结果。

7. URL 级信息过滤

是代理模块常常实现的一部分，很多厂家把这个功能单独提取出来，它其实是和代理模块一起实现的。URL 过滤用来控制内部网络对某些站点的访问，如禁止访问某些站点、禁止访问站点下的某些目录、只允许访问某些站点或者其下的文件、目录等。

14.1.4 防火墙的局限性与脆弱性

在谈到网络安全时，许多人首先会想到“防火墙”。最近几年，在稍具规模的局域网络中，防火墙都得到了广泛的部署，技术人员一般采用防火墙作为安全保障体系的第一道防线，防御黑客攻击。但是，随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙已经无法满足企业的安全需要。

1. 防火墙的局限性

防火墙的局限性主要表现在以下几个方面。

- 防火墙作为访问控制设备，无法检测或拦截嵌入到普通流量中的恶意攻击代码，比如针对 Web 服务的 Code Red 蠕虫等。
- 有些主动或被动的攻击行为是来自防火墙内部的，防火墙无法发现内部网络中的攻击行为。
- 防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据，防火墙无法检查。
- 防火墙不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内，但绝大多数单位因为不方便，不要求防火墙防内。
- 防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全，而不能自作主张。
- 防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在一个安全的地方。
- 防火墙不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议，它便不能防止利用该协议中的缺陷进行的攻击。
- 防火墙不能防止利用服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙不能防止。
- 防火墙不能防止受病毒感染文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。
- 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。
- 防火墙不能防止内部的泄密行为。对于防火墙内部的一个合法用户主动泄密，防火墙是无能为力的。
- 防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。因此对防火墙也必须提供某种安全保护。

由于防火墙具有以上一些缺陷，所以，部署了防火墙的安全保障体系还有进一步完善的

需要。

2. 防火墙的脆弱性

防火墙的脆弱性主要表现在以下几个方面。

- 防火墙的操作系统不能保证没有漏洞。目前，还没有任何一款网络的防火墙没有操作系统。只要有操作系统（无论是 Linux 还是 Unix，无论是专用还是通用）就不能保证绝对没有安全漏洞。
- 防火墙的硬件不能保证不失效。所有的硬件都有一个生命周期，都会老化，都会发生故障，也总有失效的一天。
- 防火墙软件不能保证没有漏洞。防火墙软件也是软件，是软件就会有漏洞。
- 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议来实现的，无法解决 TCP/IP 操作的漏洞。
- 防火墙无法区分恶意命令还是善意命令。有很多命令对管理员而言，是一项合法命令，而在黑客手里就可能是一个危险的命令。
- 防火墙无法区分恶意流量和善意流量。对于 ICTU 命令而言，用作网络诊断和网络攻击，从流量上是没有差异的。
- 防火墙的安全性与多功能成反比。多功能与防火墙的安全原则是背道而驰的，功能越多，漏洞越多，安全性越差。因此，除非确信需要某些功能，否则应该使其功能最小化。
- 防火墙的安全性和速度成反比。防火墙的安全性是建立在对数据的检查之上的，检查越细越安全，但检查越细则速度越慢。
- 防火墙的多功能与速度成反比。防火墙的功能越多，对系统性能的消耗越大，功能越多，检查越多，速度越慢。
- 防火墙无法保证准许服务的安全性。防火墙准许某项服务，却不能保证该服务的安全性。准许服务的安全性问题必须由应用安全来解决。

14.2 IDS

IDS（Intrusion Detection Systems，入侵检测系统）作为一种网络安全的检测设备，依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

14.2.1 IDS 概述

不同于防火墙，IDS 入侵检测系统是一个监听设备，无需串接在任何链路中，无需网络流量流经该设备，即可检测到网络中的异常传输。事实上，IDS 就是网络中的一个窃听设备，时刻关注着网络中的数据传输。图 14-2 所示为 Cisco IDS 设备。

IDS 是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分

析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

图 14-2　Cisco IDS 设备

IDS 能够检测到的攻击类型通常包括：系统扫描（System Scanning）、拒绝服务（Deny of Service）和系统渗透（System Penetration）。IDS 对攻击的检测方法主要包括：IDS 对攻击的检测方法是被动地、实时地、在线地发现计算机网络中的攻击者、在线地发现计算机网络中的攻击者。IDS 的主要优势是监听网络流量，但又不会影响网络的性能。作为对防火墙的有益补充，IDS 能够帮助网络系统快速发现网络攻击的发生，可扩展系统管理员的安全管理能力，包括安全审计、监视、进攻识别和响应等，从而提高了信息安全基础结构的完整性，被认为是继防火墙之后的第二道安全闸门。

IDS 一般位于内部网的入口处，安装在防火墙的后面，用于检测入侵和内部用户的非法活动，提供对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前进行拦截和响应入侵处理。它可在不影响网络性能的情况下对网络进行监听，从而实现对网络的保护。

IDS 在交换式网络中的位置一般选择在：

- 尽可能靠近攻击源。
- 尽可能靠近受保护资源。

这些位置通常是：

- 服务器区域的交换机上，如图 14-3 所示。
- Internet 接入路由器之后的第一台交换机上。
- 重点保护网段的局域网交换机上。

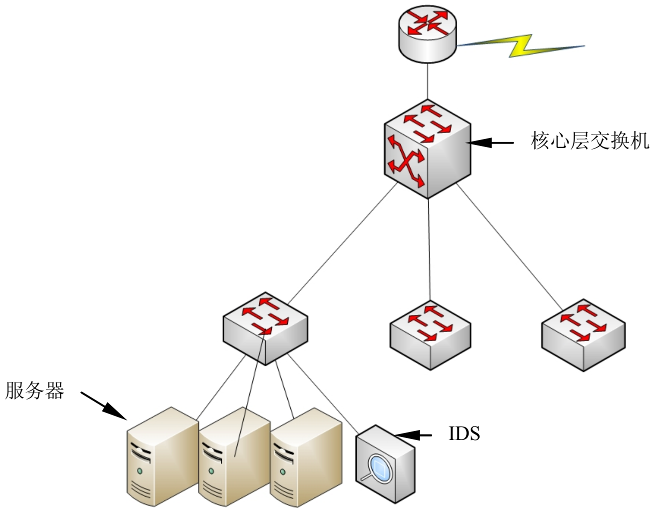


图 14-3　服务器区域的交换机上

在实际的使用中，大多数入侵检测的接入方式，都是采用 by-pass（旁路）方式来侦听网络上的数据流，所以，这就限制了 IDS 本身的阻断功能，IDS 靠发阻断数据包来阻断当前行为，并且 IDS 的阻断范围也很小，只能阻断建立在 TCP 基础之上的一些行为，如 Telnet、FTP、HTTP 等，而对于一些建立在 UDP 基础之上的行为就无能为力了。因为防火墙的策略都是事先设置好的，无法动态设置策略，缺少针对攻击的必要的灵活性，不能更好地保护网络的安全，所以 IDS 与防火墙联动的目的就是更有效地阻断所发生的攻击事件，从而使网络隐患降至较低限度。

14.2.2 IDS 优势与缺陷

IDS 本质上是一种监听系统，它依照一定的安全策略，对网络与系统的运行状况进行检测，尽可能发现、报告、记录各种攻击企图、攻击行为或者攻击结果，以保证信息系统的机密性、完整性和可用性。IDS 可分为主机型 HIDS 和网络型 NIDS，目前主流 IDS 产品均采用两者有机结合的混合型架构。

1. IDS 的优势

NIDS 使用原始网络信息作为数据源，利用运行在随机模式下的网络适配器实时监听和分析通过网络的所有通信，收集相关信息并记入日志；而 HIDS 则通常安装在被检测的主机之上，与该主机的网络实时连接，负责对系统审计日志进行智能分析和判断。若发现非法入侵或者违反统计规律的行为异常，IDS 会立即发出警报，由系统管理员进行决策处理。

IDS 的传统优势在于：

- 整体部署，实时检测，可根据用户的历史行为模型、存储在计算机中的专家知识，以及神经网络模型，对用户当前的操作进行判断，及时发现入侵事件。
- 对于入侵与异常不必作出阻断通信的决定，能够从容提供大量的网络活动数据，有利于在事后入侵分析中评估系统关键资源和数据文件的完整性。
- 独立于所检测的网络，黑客难于消除入侵证据，便于入侵追踪与网络犯罪取证。
- 同一网段或者一台主机上一般只需部署一个检测点就近检测，速度快，成本低。

入侵检测是一门综合性技术，既包括实时检测技术，也有事后分析技术。尽管用户希望通过部署 IDS 来增强网络安全，但不同的用户需求也不同，也由于攻击的天然不确定性，单一的 IDS 产品可能无法做到面面俱到。因此，IDS 的未来发展必然是多元化的。只有通过不断改进和完善技术才能更好地协助网络进行安全防御。

2. IDS 的缺陷

防火墙是一种基于访问控制的安全设备，它只能针对协议、端口和地址等信息禁止或允许某些特定的数据包经过，如果某种攻击巧妙地利用了合法途径，就可以长驱直入，视防火墙如“无物”，如通过 HTTP 协议传播的蠕虫等。IDS 虽然对所监控网段内的数据包进行分析，但检测效果还远不尽人意，目前很难检测到新出现的攻击行为，即便是已知的攻击，特征匹配也经常会出现漏报现象。误报问题就更突出了。IDS 产品的报警消息太多，其中大部分的报警消息都属于误报，即把一些正常的网络活动当成了入侵，所以海量的虚假报警消息反倒把真实有用的报警信息给淹没了，安全管理员根本无暇、也无法从中仔细挖掘出真实的入侵信息。此

外，更重要的是，IDS 主要负责检测，其响应能力有限，而被动侦听的特性决定了它的检测总是滞后于入侵的发生，对入侵的防御和阻止就更慢了一拍。

IDS 的缺陷主要包括以下几个方面。

- 检测范围不够广。虽然很多厂商都竭力吹嘘自己产品所采用的先进技术，但很少有哪家厂商能将特征检测、异常检测、拒绝服务攻击检测无缝地集成到一起，实现对已知攻击、新攻击和 DDoS/DoS 攻击的检测。
- 检测效果不理想。主要指检测的准确度，IDS 检测引擎最大的问题莫过于漏报和误报，很多 IDS 一天就能发出上千条虚假报警信息，让人目不暇接，而漏报的后果就更严重了。
- 无力防御 UDP 攻击。IDS 只能靠发阻断数据包来阻断建立在 TCP 基础上的攻击，对于建立在 UDP 基础之上的入侵则无能为力。
- 只能检测，不能防御。IDS 旁路在网络上，当它检测出黑客入侵攻击时，攻击已到达目标造成损失。IDS 无法有效阻断攻击，比如蠕虫爆发造成企业网络瘫痪，IDS 无能为力。一个理想的安全防护产品必须引入主动的入侵防御能力，在敌人入侵前就将其击退或消灭，这也反映了当前和未来的市场需求。
- 无法把攻击防御在网络之外。蠕虫、病毒、DDoS 攻击、垃圾邮件等混合威胁越来越多，传播速度加快，留给人们响应的时间越来越短，使用户来不及对入侵作出响应，往往造成企业网络瘫痪。
- 过分依赖检测主机。由于 HIDS 安装于检测主机之上，不仅消耗检测对象的部分资源，影响到被检测主机的效率，而且还必须针对不同的主机及其系统环境设计和安装各自的 HIDS。
- 性能有待提高。很多 IDS 都是 PC 服务器硬件平台上运行的软件程序，而数据包的捕获、处理、分析都需要大量的计算，即使在窄带网络上，也会出现丢包、延时太长而导致检测不准确等问题。
- 伸缩性欠佳。大部分 IDS 的监控对象是小型网络，对于大中型企业和政府网络而言，其带宽通常是数百兆位甚至千兆位，监控区域众多，需要更多的探测器，这些都超出了现在 IDS 设计之初的系统限制。
- 部署难度大。IDS 需要被放置在组织网络的重要系统和服务器的所有入口处，如果配置不当，性能和效果就会大打折扣，安全管理员还需对 IDS 特征库进行频繁地升级。显然，这将浪费大量的资源和时间。
- 安全策略不够丰富。大部分 IDS 系统只使用一个安全策略，当监控的网络包括许多不同的域或组时（如财务、市场、研发、人事等部门），需要针对不同部门制订不同的安全策略。

由于 IDS 检测引擎基于特征检测，需要源源不断地向特征库中增加新的“特征”，以增强系统对入侵的检测能力。同时，基于混杂模式的被动侦听检测体系，从本质上决定了 IDS 无法在入侵产生危害之前将其有效、可靠地阻止。IDS 存在很多缺陷，而这些缺陷使一些用户逐渐对它产生了怀疑。所以，很多安全专家认为，价值不菲的 IDS 对于企业网络安全的真正作用如同“马其诺防线”，貌似固若金汤，实际上根本无法阻挡经验丰富的攻击者，形同虚设。

14.2.3 IDS 与防火墙联动

防火墙是实施访问控制策略的系统，对流经的网络流量进行检查，拦截不符合安全策略的数据包。入侵检测系统（IDS）通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警。防火墙和 IDS 之间是互补的关系，两者协同工作，如图 14-4 所示。

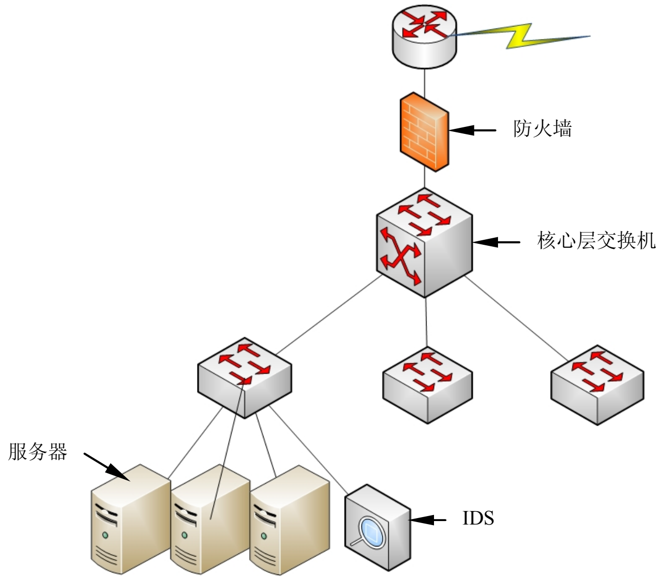


图 14-4　IDS 与防火墙协同工作

客户一般会在出口部署防火墙来进行访问控制，部署入侵检测系统来检测攻击。但是，防火墙不能有效检测并阻断夹杂在正常流量中的攻击代码，比如针对 Web 服务的 Unicode 攻击，而蠕虫爆发往往首先让防火墙瘫痪，对于 P2P 下载防火墙同样无能为力。入侵检测系统虽然能够检测到攻击，但是它提供的与防火墙联动、TCP 复位都存在很大的问题，在现实应用中很难起到相应的作用。结果是虽然看到了攻击，但仍然让攻击得手了。由此可见，借助防火墙和 IDS 的安全措施并不能完全解决现实问题。

IDS 在捕捉到某一攻击事件后，按策略进行检查，如果策略中对该攻击事件设置了防火墙阻断，那么 IDS 就会发给防火墙一个相应的动态阻断策略，防火墙根据该动态策略中的设置进行相应的阻断，阻断的时间、阻断时间间隔、源端口、目的端口、源 IP 和目的 IP 等信息，完全依照 IDS 发出的动态策略来执行。一般来说，很多情况下，不少用户的防火墙与 IDS 并不是同一家的产品，因此在联动的协议上面大都遵从 OPSEC 或者 TOPSEC 协议进行通信，不过也有某些厂家自己开发相应的通信规范。总的来说，联动有一定效果，但是稳定性不理想，特别是攻击者利用伪造的包信息，让 IDS 错误判断，进而错误指挥防火墙将合法的地址无辜屏蔽掉。

TCP 重置的缺陷：

- 只对 TCP 连接起作用。
- IDS 向攻击者和受害者发送 TCP Reset 命令，IDS 必须在 40 亿字节的范围内猜测到达受害者时的序列号数，以关闭连接。这种方法在实际上是不可实现的。

- 即使 IDS 最终猜测到了到达受害者的序列号，关闭了连接，攻击实际上已经对受害者产生了作用。

IDS 与防火墙联动的缺点：

- 使用、设置上复杂，影响 FW 的稳定性与性能。
- 阻断来自源地址的流量，不能阻断连接或单个数据包。
- 黑客盗用合法地址发起攻击，造成防火墙拒绝来自该地址的合法访问。
- 可靠性差，实际环境中没有实用价值。

因为诸多不足，在目前而言，IDS 主要起的还是监听记录的作用。用个比喻来形容：网络就好比一片黑暗，到处充满着危险，冥冥中只有一个出口。IDS 就像一支手电筒，虽然手电筒不一定能照到正确的出口，但至少总比没有要好一些。称职的网管，可以从 IDS 中得到一些关于网络使用者的来源和访问方式，进而依据自己的经验进行主观判断（注意，的确是主观判断。例如，用户连续 ping 了服务器半个小时，到底是意图攻击，还是无意中的行为？这都依据网络管理员的主观判断和网络对安全性的要求来确定对应方式）。对 IDS 的选择，跟上面谈到的防火墙的选择类似，根据自己的实际要求和使用习惯，选择一个自己够用的，会使用的就足够了。

14.3 IPS

IPS（Intrusion Prevention System，入侵防御系统）的设计基于一种全新的思想和体系架构，工作于串联（IN-LINE）方式，采用 ASIC、FPGA 或 NP（网络处理器）等硬件设计技术实现网络数据流的捕获，检测引擎综合特征检测、异常检测、DoS/DDoS 检测、缓冲区溢出检测等多种手段，并使用硬件加速技术进行深层数据包分析处理，能高效、准确地检测和防御已知、未知的攻击及 DoS/DDoS 攻击，并实施多种响应方式，如丢弃数据包、终止会话、修改防火墙策略、实时生成警报和日志记录等，突破了传统 IDS 只能检测不能防御入侵的局限性，提供了一个完整的入侵防护解决方案。

14.3.1 IPS 概述

说起网络安全，相信所有使用过网络的人都不陌生，大都遇到过下面这些情况。

- 没有及时安装新发布的一个安全补丁，造成服务器宕机，网络中断。
- 蠕虫病毒爆发，造成网络瘫痪，无法网上办公，邮件收不了，网页打不开。
- 个别用户使用迅雷、BT、电驴等 P2P 软件下载电影、电视剧、软件或 MP3，造成上网速度奇慢无比。
- 个别用户沉迷在 QQ 或 MSN 上聊天，或者《玩魔兽世界》、《穿越火线》、《跑跑卡丁车》、《天龙八部》等网络游戏，或者看在线视频，不专心工作。
- 由于个别用户的计算机被植入间谍软件，导致网络内部的机密资料被窃。
- 公司 Web 服务器遭受 SQL 注入攻击，造成公司主页内容被篡改。
- 部分员工计算机成为僵尸网络的“肉机”，向外网发起 DoS/DDoS 攻击，被有关安全部门调查。

根据调查数据显示，以上事件呈逐年上升趋势，给企业造成越来越大的直接和间接损失。

对于上述威胁，传统的安全手段（如防火墙、IDS 系统）都无法有效进行阻止。

传统的防火墙旨在拒绝那些明显可疑的网络流量，但仍然允许某些流量通过，因此防火墙对于很多入侵攻击仍然无计可施，而绝大多数 IDS 系统都是被动的，不是主动的。也就是说，在攻击实际发生之前，它们往往无法预先发出警报。而入侵防御系统 IPS 则倾向于提供主动防御，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS 是通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。如图 14-5 所示为 Cisco IPS 设备。

图 14-5　Cisco IPS 设备

IPS 之所以能够实现实时检查和阻止入侵，在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。IPS 数据包处理引擎是专业化订制的集成电路，可以深层检查数据包的内容。如果有攻击者利用二层至七层的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对三层或四层进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐一字节地检查数据包。所有流经 IPS 的数据包都被分类，分类的依据是数据包中的报头信息，如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

针对不同的攻击行为，IPS 需要不同的过滤器。每种过滤器都设有相应的过滤规则，为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤准确性。

过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。这种硬件加速技术对于 IPS 具有重要意义，因为传统的软件解决方案，必须串行进行过滤检查，因而会导致系统性能大打折扣。

14.3.2 IPS 的技术特征

作为信息安全保障主动防御的核心技术，IPS 一般应具有下列主要的技术特征。

■ **完善的安全策略**

要完整体现 IPS 的设计思想，以达到信息安全保障主动防御的目的，必须有较为完善的安全策略。安全策略分为检测策略和响应策略。检测策略提出对病毒、入侵、攻击，以及可

疑行为的检测要求；响应策略则给出各种检测方式的通信机制、联动手段、响应时机和方式等具体要求。

■ **嵌入式运行模式**

为了实现实时的深度安全防护，IPS 多采取嵌入模式运行。可根据实际需要将 IPS 嵌入到服务器、关键主机、路由器、以太网交换机等网络设备中，实现信息系统高强度实时积极防护。

■ **丰富的入侵检测手段**

信息系统综合威胁的不断发展，需要多层、深度的防护才能有效，而单一的防护措施则无能为力。为了达到联动和高效检测的目的，IPS 必须建立丰富且尽量完备的病毒特征库和入侵特征库。在检测手段上，需将基于特征的方法与基于统计的方法相结合。同时，应采取智能化的方法来提高对未知病毒或未知模式攻击的预警能力。在可能的条件下，还应当考虑网络整体的安全态势和威胁评估的分析结果，来提高检测能力。同样重要的是，IPS 将对信息系统安全造成威胁的各类因素（如病毒、入侵行为等）的检测与分析融合起来，强调对安全构成威胁的因素进行实时防护，为综合防范提供了基本前提。

■ **强大的响应功能**

这是 IPS 区别于 IDS 的最显著特点。IPS 响应一般可分为被动响应和主动响应两种类型。被动响应同传统的 IDS 响应相类似，主要是记录和报告检测出的问题，包括通知、报警，以及 SNMP 陷阱等。主动响应则是根据检测结果阻断入侵或延缓入侵进程以降低损失，一般由系统自动执行或用户驱动，这样可达到对入侵者采取行动、修正系统环境或收集有用信息的目的。此外，IPS 还可以根据策略配置，分别采取实时、近期和长期的（包括本地和全局的）响应行为。

■ **高效的运行机制**

由于 IPS 在信息安全保障体系中的重要地位，它的运行效率对于信息系统的服务质量来说至关重要。一方面，从硬件实现上，可以通过自定义硬件（网络处理器和专用 ASIC 芯片等）来提高 IPS 的运行效率；另一方面，从软件和算法实现上，通过采用信息融合和主动数据库等技术来提高推理（分析）机的运行速度，进而提高检测效率。

■ **较强的自身防护能力**

主动防御和深度防护的使命，将 IPS 推到了信息安全对抗的最前沿。在实际应用中，IPS 是一类工作在对抗网络环境下具有“指挥控制网络防御”特点的软件系统，必须考虑在攻防对抗环境下的自身生存问题。一般应从体系和软件（包括算法）两个层面来综合考虑建立 IPS 的自身防护体系，在技术途径上，采用冗余保护、通信保密、进程隐藏、综合防护等方法来构建上述体系。同时，应当强调技术与管理并重，把管理放到一个突出重要的位置，以确保 IPS 的自身生存能力。

14.3.3 IPS 的分类

IPS 大致可以分为以下几类。

■ **基于主机的入侵防御(HIPS)**

（Host-based Intrusion Prevention System，HIPS）通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统及应用程序。基于主机的入侵防御能够保护服务器的安全弱点不被不法分子所利用，因此它们在防范蠕虫病毒的攻击中起到了很好的防御作用。基于主机的入侵防御技术，可以根据自定义的安全策略，以及分析学习机制来阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库，以及其他试图从操作系统夺取控制权的入侵行为，整体提升主机的安全水平。

在技术上，HIPS 采用独特的服务器保护途径，利用由包过滤、状态包检测和实时入侵检测组成分层防御体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，既可以软件形式嵌入到应用程序对操作系统的调用当中。通过拦截针对操作系统的可疑调用，提供对主机的安全防御。也可以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。

由于 HIPS 工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用和资源的未授权的任何非法访问。HIPS 与具体的主机/服务器操作系统平台紧密相关，不同的平台需要不同的软件代理程序。

■ **基于网络的入侵防御(NIPS)**

（Network-based Intrusion Prevention System，NIPS）通过检测流经的网络流量，提供对网络系统的安全保护。由于它采用在线连接方式，所以一旦辨识出入侵行为，NIPS 就可以去除整个网络会话，而不仅仅是复位会话。同样由于实时在线，NIPS 需要具备很高的性能，以免成为网络的瓶颈，因此 NIPS 通常被设计成类似于交换机的网络设备，提供线速吞吐速率，以及多个网络端口。

NIPS 必须基于特定的硬件平台，才能实现千兆位级网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为 3 类：一类是网络处理器（网络芯片）；一类是专用的 FPGA 编程芯片；第三类是专用的 ASIC 芯片。

在技术上，NIPS 吸取了目前 NIDS 所有的成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是最广泛应用的技术，具有准确率高、速度快的特点。基于状态的特征匹配不但检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。

协议分析是一种较新的入侵检测技术，它充分利用网络协议的高度有序性，并结合高速数据包捕捉和协议分析，来快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段。协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，来寻找可疑的或不正常的访问行为。协议分析不仅仅基于协议标准（如 RFC），还基于协议的具体实现，这是因为很多协议的实现偏离了协议标准。通过协议分析，IPS 能够针对插入与规避攻击进行检测。异常检测的误报率比较高，NIPS 不将其作为主要技术。

■ **应用入侵防御（AIP）**

NIPS 产品有一个特例，即应用入侵防御（Application Intrusion Prevention，AIP），它把基于主机的入侵防御扩展成为位于应用服务器之前的网络设备。AIP 被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设定好的安全策略，保护服务器的安

全。NIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

NIPS 的实时检测与阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防御功能。

14.3.4 IPS 的优势与作用

入侵防御系统作为一种在线部署的产品，提供主动的、实时的防护，其设计目标旨在准确检测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地在检测到恶意流量的同时或之后才发出告警。IPS 是通过直接串联到网络链路中而实现这一功能的，即 IPS 接收到外部数据流量时，如果检测到攻击企图，就会自动地将攻击包丢掉或采取措施将攻击源阻断，而不把攻击流量放进内部网络。

1. IPS 的技术优势

实时检测与主动防御是 IPS 最为核心的设计理念，也是其区别于防火墙和 IDS 的立足之本。为实现这一理念，IPS 在如下几个方面实现了技术突破，形成了不可低估的优势。

■ **在线安装（In-Line）**

IPS 保留 IDS 实时检测的技术与功能，但是却采用了防火墙式的在线安装，即直接嵌入到网络流量中，通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。

■ **实时阻断（Real-time Interdiction）**

IPS 具有强有力的实时阻断功能，能够预先对入侵活动和攻击性网络流量进行拦截，避免其造成任何损失。

■ **先进的检测技术（Advanced Detection Technology）**

主要是并行处理检测和协议重组分析。所谓并行处理检测，是指所有流经 IPS 的数据包，都采用并行处理方式进行过滤器匹配，实现在一个时钟周期内，遍历所有数据包过滤器。而协议重组分析是指所有流经 IPS 的数据包，必须首先经过硬件级预处理，完成数据包的重组，确定其具体应用协议。然后，根据不同应用协议的特征与攻击方式，IPS 对于重组后的包进行筛选，将可疑者送入专门的特征库进行比对，从而提高检测的质量和效率。

■ **特殊规则植入功能（Build-in Special Rule）**

IPS 允许植入特殊规则以阻止恶意代码。IPS 能够辅助实施可接收应用策略（AUP），如禁止使用对等的文件共享应用和占有大量带宽的免费因特网电话服务工具等。

■ **自学习与自适应能力（Self-study & Self-adaptation Ability）**

为了应对黑客们处心积虑、花样翻新的攻击手段，IPS 必须具有人工智能的自学习与自适应能力。能够根据所在网络的通信环境和被入侵状况，分析和抽取新的攻击特征以更新特征库，自动总结经验，订制新的安全防御策略。

2. IPS的主要作用

从IPS的工作原理来看，IPS，有以下几个主要作用。

■ **为网络提供“虚拟补丁”**

IPS预先自动拦截黑客攻击、蠕虫、网络病毒、DDoS等恶意流量，使攻击无法到达目的主机，这样即使没有及时安装最新的安全补丁，企业网络仍然不会受到损失。IPS给企业提供了时间缓冲，在厂商就新漏洞提供补丁和更新之前确保企业的安全。

■ **进行“流量净化”**

目前企业网络的带宽资源经常被严重占用，主要是在正常流量中夹杂了大量的非正常流量，如蠕虫病毒、DoS攻击等恶意流量，以及P2P下载、在线视频等垃圾流量，造成网络堵塞。IPS可以过滤正常流量中的恶意流量，同时对垃圾流量进行控制，为网络加速，还企业一个干净、可用的网络环境。

■ **加强“内容管理”**

随着网络安全向更高层次的发展，对网络内容的管理和控制得到了认可和加强。IPS提供对面向应用层和内容层的网络内容的安全防护，可以检测并阻断间谍软件、木马后门，并可以对即时通信软件、在线视频等的内容进行监控及阻断。

14.3.5 IPS的缺陷

IPS技术的缺陷主要包括4个方面，即单点故障、性能瓶颈、误报与漏报和总体拥有成本较高。

■ **单点故障（Single-point Fault）**

设计要求IPS必须以嵌入模式工作在网络中，而这就可能造成瓶颈问题或单点故障。如果IDS出现故障，最坏的情况也就是造成某些攻击无法被检测到，而嵌入式的IPS设备出现问题，就会严重影响网络的正常运转。如果IPS出现故障而关闭，用户就会面对一个由IPS造成的拒绝服务问题，所有客户都将无法访问企业网络提供的应用。

■ **性能瓶颈（Performance Bottle-neck）**

由于IPS往往被串联于网络出口（如图14-6所示），因此，即使IPS设备不出现故障，它仍然是一个潜在的网络瓶颈，不仅会增加滞后时间，而且会降低网络的效率。IPS必须与数千兆位或者更大容量的网络流量保持同步，尤其是当加载了数量庞大的检测特征库时，设计不够完善的IPS嵌入设备无法支持这种响应速度。因此，绝大多数高端IPS产品供应商都通过使用自定义硬件（FPGA、网络处理器或者ASIC芯片）来提高IPS的运行效率，以减少其对于业务网络的负面影响。

■ **误报（False positive）与漏报（False negatives）**

误报率和漏报率也需要IPS认真面对。在繁忙的网络当中，如果以每秒需要处理10条警报信息来计算，IPS每小时至少需要处理3万多条警报，一旦生成了警报，最基本的要求就是IPS能够对警报进行有效处理。如果入侵特征编写得不是十分完善，那么“误报”就有了可乘

之机，导致合法流量也有可能被意外拦截。对于实时在线的 IPS 来说，一旦拦截了“攻击性”数据包，就会对来自可疑攻击者的所有数据流进行拦截。如果触发了误报警报的流量恰好是来自上级、合作伙伴和客户的重要信息，IPS 不仅实施了一次错误阻断，而且会切断与他们的信息通道，其结果不言而喻。

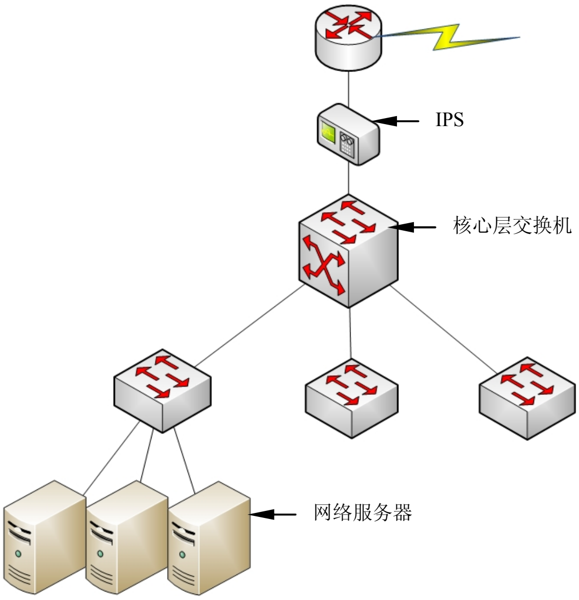


图 14-6　IPS 串联于网络出口

■　**总体拥有成本（TOC）高**

为了避免由单点故障而导致的网络连接中断，需要采用高可用性（HA，High Availability）结构，而浩大的高可用性实时计算需求，决定了 IPS 必须选用高端的专用计算设备，但可观的总体拥有成本（Total Cost of Ownership，TOC）却使不少用户望而却步。

14.3.6 部署 IPS

IPS 支持多种工作模式，便于管理员分阶段、有步骤地部署实施。

第 1 阶段　只检测，不防御。

如同 IDS 一样，IPS 接在 SPAN 端口（Switched Port Analyzer，监控端口）或 TAP 设备（Test Access Point，测试访问点），被动监控网络流，这个阶段 IPS 的任务是适应环境，只检测，不主动防御。

第 2 阶段　串联检测，但不防御。

IPS 以串联方式工作，但仍只进行检测，不阻断数据流，但它会将不符合协议的数据包丢弃，确保通过的数据包都是合乎规范的，使插入和规避类攻击无从得手。在这个阶段，让管理员知道 IPS 在保护网络和业务的同时不会产生新的麻烦。例如，假设管理员一上来就将 IPS 设置为防御方式，当 IPS 将一些合法的数据包错判为攻击并实施阻断时，IPS 就沦为了 DoS 工具，这显然是不行的，所以先给 IPS 一个学习的过程是很有必要的。

第 3 阶段　检测，并有选择地防御。

当串联方式被证明合适后，管理员就可以根据报警日志确定入侵检测策略的有效性，它可以先选择一些最严重的报警，确保没有误报，然后对该类型的特征实施阻断响应。在此阶段，IPS 检测攻击并有选择地防御，只将有明显危害的攻击流阻断。

第 4 阶段　检测，并全面防御。

当 IPS 的有效性获得认可并且安全策略经过不断的调整优化之后，安全管理员就可以为一切特征（证明其不会产生误报）设置响应方式，从而使 IPS 进入全面的防御工作模式，一旦发现有害数据包就将其丢弃并阻断随后的数据流。

提・示

IPS 的串联工作方式也存在一定的问题，虽然底层采用专用硬件电路设计，但 IPS 仍有可能影响网络性能和可靠性，“零丢包”、“零延时”只是理想状况，如果 IPS 停止运转后线路仍畅通，则相当于没有任何防御效果；如果停止运转后线路断掉，企业网络就与外部网路完全切断，IPS 反倒成了产生拒绝服务攻击的替罪羊。此外，同 IDS 一样，IPS 的检测效果也有待提高，要将漏报和误报率降低到尽可能低的程度，报警处理机制、集中管理和配置、规则定义、部署、特征库优化等方面也还要做大量的工作。

第 15 章　防火墙的选择与适用

黑客就像身边的空气一样无处不在，即使是再严密的系统，只要暴露在网络中就随时都有被攻击的可能。所以，防火墙的目的并不是用来维护已经受到入侵的用户，而是防患于未然，是每一个计算机网络，甚至每一台计算机都必备的工具。目前，网络防火墙市场缺少规范，产品性能和质量参差不起，给用户的选择造成了一定的困难。

15.1　防火墙的主要参数

网络防火墙和前面介绍的路由器非常类似，是一台特殊的计算机，同样有自己的硬件系统和软件系统，和一般计算机相比只是没有独立的输入和输出设备。防火墙的重要参数主要包括性能参数和功能参数两个方面。

15.1.1　防火墙的性能参数

防火墙的主要性能参数是指影响网络防火墙包处理能力的参数，包括以下几个方面。

■　**设备类型**

防火墙的分类也是比较复杂的，如企业级防火墙、边界防火墙、个人防火墙等，不同类型的防火墙具有各自不同的功能，当然价格和管理方面也会有所差异。

■　**系统硬件**

防火墙硬件参数是指设备使用的处理器类型或芯片及主频，内存容量，闪存容量，网络接口，存储容量类型等数据，一般而言高档防火墙的硬件性能优越，处理器在 600 MHz 左右，内存可以达到 256 MB。

■　**并发连接数**

并发连接数是衡量防火墙性能的一个重要指标，是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，这个参数的大小直接影响到防火墙所能支持的最大信息点数。

> **提·示**　低端防火墙的并发连接数都在 1000 个左右，而高端设备则可以达到数万甚至数 10 万个并发连接。

■ **虚拟专用网络支持**

目前大多数防火墙产品都支持这种功能，可以通过特殊的加密的通信协议在连接到Internet上的位于不同地方的两个或多个企业内部网之间，建立一条专有的通信线路。就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。

■ **吞吐量**

防火墙的主要功能就是对每个网络中传输的每个数据包进行过滤，因此需要消耗大量的资源。吞吐量是指在不丢包的情况下单位时间内通过防火墙的数据包数量。

随着Internet的日益普及，内部网用户访问Internet的需求在不断增加，一些企业也需要对外提供诸如WWW页面浏览、FTP文件传输、DNS域名解析等服务，这些因素会导致网络流量的急剧增加，而防火墙作为内外网之间的唯一数据通道，如果吞吐量太小，就会成为网络瓶颈，给整个网络的传输效率带来负面影响。因此，考察防火墙的吞吐能力有助于更好地评价其性能表现。这也是测量防火墙性能的重要指标。

> **提·示** 吞吐量的大小主要由防火墙内网卡，及程序算法的效率决定，尤其是程序算法，会使防火墙系统进行大量运算，通信量大打折扣。因此，大多数防火墙虽号称100 Mbps防火墙，由于其算法依靠软件实现，通信量远远没有达到100 Mbps，实际只有10～20 Mbps。纯硬件防火墙，由于采用硬件进行运算，因此吞吐量可以达到线性90～95 Mbps，是真正的100 Mbps防火墙。

■ **安全过滤带宽**

安全过滤带宽是指防火墙在某种加密算法标准下的整体过滤功能，如DES（56位）算法或3DES（168位）算法等。一般来说，防火墙总的吞吐量越大，其对应的安全过滤带宽越高。

■ **支持用户数**

防火墙的用户数限制分为固定限制用户数和无用户数限制两种。前者比如SOHO型防火墙一般支持几十到几百个用户不等，而无用户数限制大多用于大的部门或公司。这里的用户数量和前面介绍的并发连接数并不相同，并发连接数是指防火墙的最大会话数（或进程），而每个用户可以在一段时间里产生很多连接。

15.1.2 防火墙的功能参数

防火墙的功能参数，主要是指防火墙可以实现哪些与网络安全相关的功能。主要包括以下几个方面。

■ **入侵检测**

入侵检测（ID）是指防火墙依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

■ **安全标准**

安全标准一般有两种形式：一种是专门的特定的安全标准；另一种是在产品标准或工艺标准中列出有关安全的要求和指标。安全标准一般均为强制性标准，由国家通过法律或法令形式规定强制执行。网络与信息安全标准则是在计算机网络领域通用的一种安全标准，不同性能的防火墙归属的安全标准也是不一样的。

■ **防火墙端口**

防火墙的控制端口通常为Console端口，防火墙的初始配置也是通过控制端口（Console）与PC（通常是便于移动的笔记本电脑）的串口（RS-232）连接，再通过Windows系统自带的超级终端（HyperTerminal）程序进行选项配置。其实防火墙还可以通过其他方式进行配置，如Telnet、TFTP服务器等。

■ **远程管理**

防火墙管理是指对防火墙具有管理权限的管理员行为和防火墙运行状态的管理，管理员的行为主要包括：通过防火墙的身份鉴别，编写防火墙的安全规则，配置防火墙的安全参数，查看防火墙的日志等。

管理界面一般用来完成对防火墙的配置、管理和监控。管理界面设计直接关系到防火墙的易用性和安全性。防火墙主要有两种远程管理界面，即Web界面和GUI界面。对于硬件防火墙，一般还有串口配置模块或控制台控制界面。GUI 界面可以设计得比较美观和方便，并且可以自定义协议，被多数厂商使用。Web界面也有厂商使用，不过要增加一个CGI解释部分，所以减少了防火墙的可靠性。部分厂家还增加了校验功能，即系统会自动识别用户配置上的错误，防止因配置错误而造成的不安全隐患。

■ **代理**

目前主要由两种方式实现防火墙的代理功能，即透明代理（Transparent Proxy）和传统代理，二者的工作原理如表15-1所示。

表15-1　代理防火墙的分类

透明代理（Transparent proxy）	实质上它属于DNAT的一种，它主要指内网主机需要访问外网主机时，不需要做任何设置，完全意识不到防火墙的存在，而完成内外网的通信。但其基本原理是防火墙代替内部网络主机完成与外部网络主机的通信，然后把结果反馈给内部网络主机，在这个过程中，无论内部主机还是外部主机都意识不到它们其实是在和防火墙通信。而从外部网络只能看到防火墙，这就隐藏了内部网络，提高了安全性
传统代理	其工作原理与透明代理相似，所不同的是它需要在客户端设置代理服务器。因此这种方式安全性好，但效率低

■ **审计和报警机制**

结合网络配置和安全策略对防火墙的相关数据分析完成以后，就要作出接受、拒绝、丢弃或加密等决定。如果要通过防火墙的数据违反了安全策略，审计和报警机制就会开始起作用，并记录和报告。审计是一种重要的安全措施，用以监控通信行为和完善安全策略，检查安全漏洞和错误配置。报警机制是在通信违反相关策略以后，以多种方式如声音、邮件、电话、手机短信息及时报告给管理人员。

日志由于数据量比较大，主要通过两种方式解决，一种是将日志挂接在内部网络的一台

专门存放日志的日志服务器上；一种是将日志直接存放在防火墙本身的存储器中。日志单独存放这种方式配置较为麻烦，然而可以存放的日志量却很大；日志存放在防火墙中时，无需做额外配置，然而由于防火墙容量有限，所存放的日志量往往较小。

> **提·示** 防火墙的审计和报警机制在防火墙体系中有很重要的作用，只有有了审计和报警，管理人员才可能知道网络是否受到攻击。另外，防火墙的该功能也有很大的发展空间，如日志的过滤、提取、简化等。日志还可以进行统计、分析、（按照特征）、存储（在数据库中），稍加扩展便又是一个网络分析与查询模块。

■ **MAC与IP地址的绑定**

MAC与IP地址绑定起来，主要用于防止受控（不可访问外网）的内部用户通过更换IP地址访问外网。因为它实现起来太简单了，内部只需要两个命令就可以实现，所以绝大多数防火墙都提供了该功能。

■ **多级过滤技术**

采用多级过滤措施，在网络层，过滤掉所有的源路由分组和假冒的IP源地址；在传输层，遵循过滤规则，过滤掉所有禁止出入的协议和有害数据包；在应用层，能利用FTP、SMTP等各种网关，控制和监测Internet提供的所有通用服务。

■ **杀毒技术**

部分防火墙集成了病毒防火墙功能，与专用的硬件网络防病毒设备类似，实现病毒的过滤和预防，不让病毒肆虐横行。

15.2 防火墙的分类与适用

目前，市场上防火墙的种类可谓是多种多样，无论是性能还是价格都存在着较大的差异。防火墙的分类标准也是比较复杂的，接下来我们介绍当前比较流行的几种分类标准。

15.2.1 按照软硬件形式划分

按照软硬件形式是最明显的划分标准，按照这种方式可以将防火墙划分为软件防火墙和硬件防火墙两种。

1. 硬件防火墙

硬件防火墙的硬件和软件都单独进行设计，由专用网络芯片处理数据包。同时，采用专门的操作系统平台，从而避免通用操作系统的安全性漏洞。并且对软硬件的特殊要求，使硬件防火墙的实际带宽与理论值基本一致，有着高吞吐量、安全与速度兼顾的优点。从外观上看，硬件防火墙和交换机、集线器差不多，也是许多计算机网络中必备的网络设备。但是，防火墙不会像其他网络设备那样提供多个连接端口，一般只有少数的几个端口，分别用于连接内部网络和外部网络。图15-1所示为Cisco ASA 5580自适应防火墙。

图 15-1　Cisco ASA 5580 自适应防火墙

2.　软件防火墙

软件防火墙是安装在 PC 平台上的软件产品，它通过在操作系统底层工作来实现网络管理和防御功能的优化。例如，Microsoft Forefront TMG（如图 15-2 所示）就是一款非常典型的软件防火墙。当然，尽管许多网络防火墙都号称是硬件防火墙，并且硬件连同软件一起销售，但并没有自己独立的操作系统，只是基于 x86 计算机架构和开放的 Linux/UNIX 操作系统，以及一套自己开发的网络防火墙软件，其从根本意义上来讲，仍然是软件防火墙。

图 15-2　Forefront TMG 欢迎界面

硬件防火墙与软件防火墙相比较，有很多优越性，如表 15-2 所示。

表 15-2　硬件防火墙与软件防火墙相比较

比　　较	软　　件	硬　　件
安全性	OS:为通用 OS，其安全性主要取决于 OS 的安全性 从本质上看，软件防火墙既要防止来自外部网络的攻击，还要防止来自操作系统厂商的攻击 另外，就其本身而言，各种操作系统因其考虑通用性，故均做得很复杂，其安全性和各类脆弱性不断发现，作为防火墙类安全控制设备，建立于这样的系统之上，其安全性能难以提高，也给各防火墙的管理增加了很多工作量	OS：自主开发 为专用操作系统，仅服务于防火墙应用，或防火墙直接嵌在操作系统内，减少系统复杂程度，提高安全信任程度

（续表）

比　较	软　件	硬　件
应用相关性	在通用操作系统上，必然运行相关或无关的各种应用，甚至为黑客程序，各种应用在操作系统内竞占资源，共同使用操作系统的相关调用，有意或无意的应用或操作可能给防火墙应用带来安全或其他方面的影响	无其他任何应用存在
管理操作安全性	防火墙本身管理的唯一性是容易保证的，但防火墙的下层与操作系统紧密连接，如网络接口，其管理不依赖于防火墙本身，其他应用或应用管理可能会使网络接口不可用或崩溃，因此要求防火墙管理员必须熟悉系统，并精通相关应用或业务	防火墙提供专用管理接口，并有系列安全措施，管理员对系统的操作行为是唯一的、有限的，并经过严格的安全审计的
性能	通用操作系统庞大，体系完善，在其上运行的各类应用的性能必然受到很大影响	精简的操作系统，不处理无关的事务，效率很高
可靠性	软件型防火墙的运行平台为各类商业级PC或服务器，其不间断运行时间较难满足使用要求，用户需要付出较高代价购买高可靠性服务器系统，如热备份等 通用操作系统本身的稳定性受多种因素影响，其稳定性和可靠性很难管理和保证，即使UNIX系统，尽管其稳定性较高，但其受影响的面太宽，如其他应用导致的资源耗尽或系统重启动等，也会中断网络通信，影响正常业务，这对于重要和关键业务系统的影响或损失可能是很大的	使用工业级或军用级专用器件生产设备，平均无故障时间很长，真正满足使用要求，也满足成本控制要求 软件系统可靠性由本身可靠性保证，并且影响可靠性的相关因素很少
可维护性	操作系统本身的维护、防火墙本身的维护、相关或无关应用的维护均与防火墙的维护密切相关 在升级方面，相关的事务处理的难度和复杂程度也相对较高	维护相对简单，维护行为由防火墙限定，无其他相关性，时间短，可能引起的网络中断时间很短。 升级简单，时间短，行为结果唯一
管理员要求	对系统和相关应用精通，要求管理员具有较高的管理能力	熟悉防火墙的相关管理命令操作即可
应急处理适应能力	紧急情况下对处理的适应能力不高，可能导致操作系统的不可用，系统的重新安装将需很长时间	硬件设备应急处理适应能力很强，系统初始化、启动、配置、恢复、断开等均快速完成
事故责任	事故责任的相关性大，故障责任点较难确定，如操作系统、其他应用及防火墙本身	责任明确，防火墙明确承担所有安全责任

提·示　国内市场的硬件防火墙大部分都是“软硬件结合的防火墙”，即“订制机箱+X86架构+防火墙软件模块”(大多数基于Linux或UNIX系统开发)。其核心技术实际上仍然是软件，吞吐量不高，容易造成带宽瓶颈。由于PC架构本身不稳定，因此往往难以适应7×24的不间断运行。所以，这种防火墙一般只能满足中低带宽的安全要求，在高流量环境下往往会造成网络堵塞甚至系统崩溃。

15.2.2 按照实现技术划分

根据防火墙技术的不同可以将防火墙划分为数据包过滤型防火墙、应用级网关型防火墙、代理服务型防火墙和复合型防火墙。但是，也有些分类标准是将应用级网关型防火墙作为代理服务型防火墙的一种。

1. 数据包过滤型防火墙

数据包过滤（Packet Filtering）技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制表（Access Control Table）。这种防火墙只检查数据包的报头信息，而“不过问”具体的信息，依此决定是否允许数据包通过，如图 15-3 所示。这种防火墙以以色列的 Checkpoint 防火墙和美国 Cisco 公司的 PIX 防火墙最具代表性。

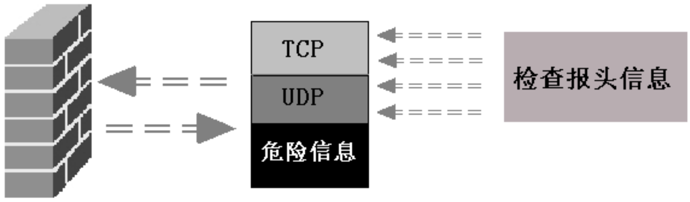


图 15-3 包过滤型防火墙拦截过程

> **提·示** 报头包括源地址、目的地址、所用的端口号、协议状态等因素，也就是图中的 TCP 和 UDP 部分。

数据包过滤型防火墙逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好，它通常安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

包过滤方式是一种通用、廉价、有效的安全手段。之所以通用，因为它不针对各个具体的网络服务采取特殊的处理方式；之所以廉价，因为大多数路由器都提供分组过滤功能；之所以有效，因为它能很大程度地满足企业的安全要求。所根据的信息来源于 IP、TCP 或 UDP 包头。

包过滤的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关，但其弱点也是明显的。

- 进行过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不可能充分满足。
- 在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响。
- 由于缺少上下文关联信息，不能有效地过滤 UDP、RPC 一类的协议，数据包的源地址、目的地址，以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒。
- 大多数过滤器中缺少审计和报警机制，且管理方式和用户界面较差，入侵者一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击。
- 对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。

2. 应用级网关型防火墙

应用级网关（Application Level Gateways）是在网络应用层上建立协议过滤和转发功能。

只检查数据包的具体数据信息，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告，如图 15-4 所示。实际中的应用网关通常安装在专用工作站系统上。

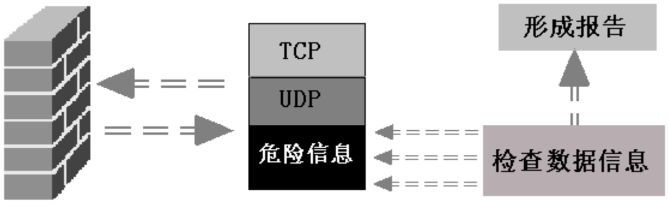


图 15-4 应用级网关型防火墙拦截过程

数据包过滤和应用级网关防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑判定是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统建立直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这有利于实施非法访问和攻击。

3. 代理服务型防火墙

代理服务（Proxy Service）也称链路级网关或 TCP 通道（Circuit Level Gateways or TCP Tunnels），也有人将它归于应用级网关一类。它是针对数据包过滤和应用级网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个终止代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。

此外，代理服务也对过往的数据包进行分析、注册登记，形成报告。同时，当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

应用代理型防火墙是内部网络与外部网络的隔离点，起着监视和隔绝应用层通信的作用。它工作在 OSI 模型的最高层，掌握着应用系统中可用作安全决策的全部信息。

4. 复合型防火墙

由于对更高安全性的要求，常把基于包过滤的方法与基于应用代理的方法结合起来，形成复合型防火墙产品，进一步基于 ASIC 架构，把防病毒、内容过滤整合到防火墙中，其中还包括 VPN、IDS 功能，并且可以在防火墙核心部分建立状态连接。维护连接，将每个数据包作为单个事件处理，如图 15-5 所示。通常包括表 15-3 所示的两种方案。

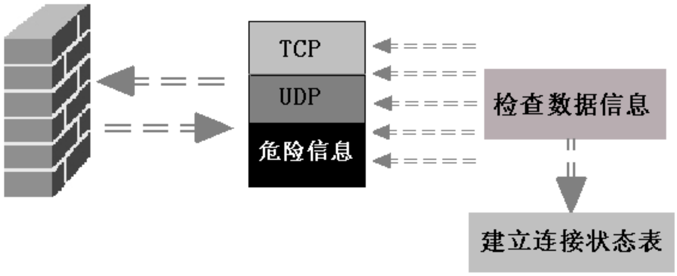


图 15-5 复合型防火墙拦截过程

表 15-3 复合型防火墙的两种方案

屏蔽主机防火墙体系结构	在该结构中，分组过滤路由器或防火墙与 Internet 相连，同时一个堡垒机安装在内部网络，通过在分组过滤路由器或防火墙上过滤规则的设置，使堡垒机成为 Internet 上其他节点所能到达的唯一节点，这确保了内部网络不受未授权外部用户的攻击
屏蔽子网防火墙体系结构	堡垒机放在一个子网内，形成非军事化区，两个分组过滤路由器放在这一子网的两端，使这一子网与 Internet 及内部网络分离。在屏蔽子网防火墙体系结构中，堡垒主机和分组过滤路由器共同构成了整个防火墙的安全基础

15.2.3 按照硬件结构划分

根据防火墙的结构不同，可以将防火墙分为单一主机防火墙、路由器集成防火墙、分布式防火墙和融合型防火墙。

1. 单一主机防火墙

单一主机防火墙既是最传统的防火墙，也是应用最为广泛的防火墙。它独立于其他网络设备，位于网络边界。这种防火墙从结构上看，与一台普通服务器主机的内部结构差不多，同样拥有 CPU、内存、硬盘、网卡等基本组件。

与普通服务器略有不同，防火墙至少集成了两个以太网卡，用于实现与内、外部网络的连接。硬盘用来存储防火墙所用的基本程序，如数据包过滤程序和代理服务器程序等，有的防火墙还把日志记录也记录在此硬盘上。虽然如此，也不能说它就与普通的 PC 一样，因为它的工作性质，决定了它要具备非常高的稳定性、实用性，具备非常高的系统吞吐性能。正因如此，看似与 PC 差不多的配置，但价格却相差甚远。图 15-6 所示为 Cisco ASA 自适应防火墙，可借助扩展卡提供丰富的网络接口。

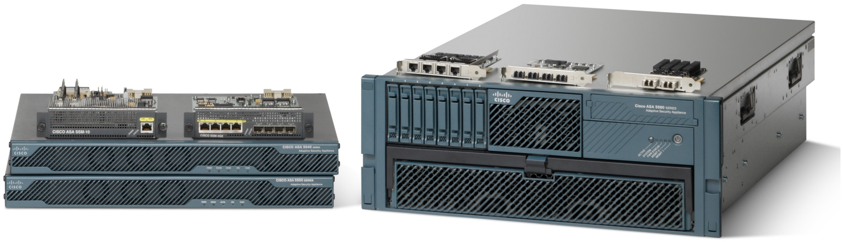


图 15-6 Cisco ASA 自适应防火墙及模块

> **提示** 单一主机防火墙的主要特点就是功能强大，工作效率高，但是价格也非常高，一般适用于大型的企业网络环境。

2. 路由器集成防火墙

这种防火墙严格来说应该是路由器或路由设备（如三层交换机）的一种，为连接的网络提供路由选择才是它的本职工作。随着防火墙技术的发展及应用需求的提高，生产商开始将单

一主机防火墙中的部分技术应用于路由器的开发设计当中，因此才产生了这种所谓的路由器集成防火墙。虽然功能远远不能与单一主机防火墙相提并论，但是应付一般的非法入侵的能力还是有的，最主要的是这种防火墙价格比较便宜，非常适用于中小型企业网络。例如，可用于Cisco Catalyst 6500系列交换机和Cisco 7600系列路由器的防火墙服务模块（FWSM），是一种高速的、集成化的防火墙，可以提供5.5 Gbps的吞吐量，每秒10万个连接，以及100万个并发连接，每个设备最高可以提供20 Gbps的吞吐量。图15-7所示为Cisco FWSM。

图15-7　Cisco FWSM

3. 分布式防火墙

分布式防火墙不再像单一主机防火墙那样是一个独立的硬件实体，而是由多个软、硬件系统组合而成。单一主机防火墙和路由器集成防火墙一般都是工作在网络边界上，但是分布式防火墙就不同了，它是渗透于网络的每一台主机中，对整个内部网络的主机实施保护。在网络服务器中，通常会安装一个用于防火墙系统管理的软件，在服务器及各主机上安装有集成网卡功能的PCI防火墙卡，这样一块防火墙卡同时兼有网卡和防火墙的双重功能，如图15-8所示。这样一个防火墙系统就可以彻底保护内部网络。各主机把任何其他主机发送的通信连接都视为“不可信”的，都需要严格过滤。而不是传统边界防火墙那样，仅对外部网络发出的通信请求“不信任”。

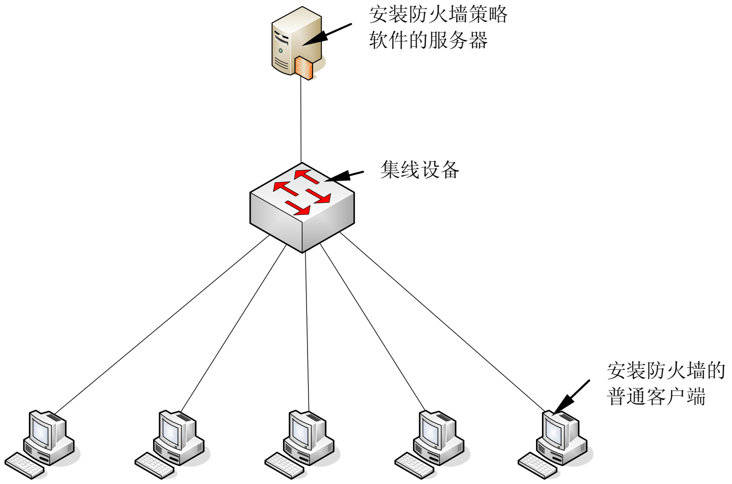


图15-8　分布式防火墙

4. 融合型防火墙

融合型防火墙能够以物理设备的方式，在同一个平台上提供融合的多功能安全和 VPN 服务。借助融合型防火墙、入侵防御系统（IPS）和网络 Anti-X 服务，网络管理员可以部署各种威胁防御和安全服务，同时满足 SSL VPN 和 IPSec 远程接入，以及站点间连接的需求。

例如，Cisco ASA 系列（如图 15-9 所示）自适应安全设备能够提供多种 VPN 和安全服务，因而能够一机多用。企业可以将其部署为单功能独立设备，也可以作为组合解决方案，根据特殊部署环境订制 Anti-X、IPS、防火墙和 VPN 应用。在小企业和分支机构环境中，Cisco ASA 5500 系列商业版还可以作为“一体化”设备，提供全面的威胁防御和 VPN 服务，并满足这种部署的预算和运营要求。

图 15-9　Cisco ASA 5500/5500-X 系列

15.2.4 按照防火墙在网络中的位置划分

按照这种分类标准又可以将防火墙划分为边界防火墙、个人防火墙和混合型防火墙。

边界防火墙也就是本章中详细介绍的硬件防火墙，一般安装在内部网络与外部网络的边界连接处，主要用来隔离内外网络，这种防火墙无论性能还是工作效率都是最高的，但是在管理员技术水平方面的要求也非常高，同时价格也较贵。

个人防火墙主要是软件防火墙，工作在每一台计算机中，只能防护本地计算机的安全工作，目前有许多防火墙软件都是共享的，所以这种防火墙基本不需要任何投资。

所谓的混合型防火墙主要是指前面介绍过的分布式防火墙或嵌入式防火墙，它本身就是一整套防火墙系统，包括若干个软件和硬件部分，分布在内外网络边界和内部网络的计算机之间，既可以对内外网络之间的数据进行过滤和拦截，又可以对网络内部的各主机间的通信进行隔离，它属于一种最新式的防火墙技术，性能最好，价格也最贵。

15.3 防火墙的选择

选择网络防火墙时，应主要考虑网络的规模、网络的架构、网络的安全需求、在网络中的位置，以及网络端口的类型等要素，选择性能、功能、结构、接口、价格都最为适宜的网络安全产品。

15.3.1 防火墙的选择策略

针对越来越多的蠕虫、病毒、间谍软件、垃圾邮件、DoS/DDoS等混合威胁及黑客攻击，不仅需要有效检测到各种类型的攻击，更重要的是降低攻击的影响，从而保证业务系统的连续性和可用性。

一个完善的网络入侵防御系统应该具备以下特征。

- 提供针对各类攻击的检测和防御功能，同时提供丰富的访问控制能力。
- 准确识别各种网络流量，降低漏报和误报率，避免影响正常的业务通信。
- 满足高性能的要求，提供强大的分析和处理能力，保证正常网络通信的质量。
- 具备良好的可靠性，提供硬件BYPASS或HA等可靠性保障措施。
- 提供灵活的部署方式，支持在线模式和旁路模式的部署，第一时间把攻击阻断在企业网络之外，同时也支持旁路模式部署，用于攻击检测，适合不同用户的需要。
- 支持分级部署、集中管理，满足不同规模网络的使用和管理需求。

15.3.2 Cisco ASA简介

ASA（Adaptive Security Appliance，适应性安全产品）是Cisco系列中全新的防火墙和反恶意软件安全产品。ASA系列产品分为两种型号，即企业版和商业版。企业版包括4种产品，即内容安全版本（Content Security Edition）、防火墙版本（Firewall Edition）、IPS版本（IPS Edition）和VPN版本（SSL/IPsec VPN Edition）。

对于网络而言，新的安全威胁层出不穷，包括病毒、蠕虫、大量应用软件（比如P2P软件、网络游戏、即时通信软件等）、网络欺诈，以及应用程序层面的攻击，等等。由于安全威胁变化多端，因此仅仅使用一台静态数据包过滤防火墙来保护网络已经远远不够了。

如果一台设备可以应付多种威胁，就称其提供了“anti-X”能力，或者说它提供了“多重威胁（multi-threat）”防护，但是一般的静态防火墙恰恰无法提供这种层次的防护。显然，大家都不希望采取安装一台静态防火墙过滤，同时再使用一些其他的安全工具来防护其他威胁的办法。因此，用户更迫切需要一台“集所有功能于一身”的设备，或是采用一台UTM（Unified Threat Management，统一威胁管理）设备。

UTM是对传统防护手段的整合和升华，是建立在原有安全网关设备基础之上的，拥有防火墙、入侵防御（IPS）、防病毒（AV）、VPN、内容过滤、反垃圾邮件等多种功能，这些技术处理方式仍然是UTM的基础，但这些处理方式不再各自为战，需要在统一的安全策略下相互配合，协同工作。

当然，对于众多的功能，有必备功能和增值功能之分。一般而言，防火墙、VPN、入侵防御、防病毒是必备的功能模块，缺少任何一个都不能称之为UTM。其余则是增值功能，用户可以根据自身需求进行选择。

Cisco ASA针对不同类型的攻击提供了防护，甚至比一台UTM设备更强劲、更有效。不过，Cisco ASA若欲成为一台真正的UTM，还需要装一个CSC-SSM模块（Content Security and Control Security Service，内容安全及控制安全服务）。该模块在ASA中提供Anti-X功能，如果没有CSC-SSM模块，那ASA的功能看起来会更像一台传统意义上的防火墙。

Cisco ASA 自适应安全设备集成了 Cisco PIX 安全防火墙、Cisco IPS 传感器和 Cisco VPN 远程安全接入的最新技术，提供了一个无与伦比的优秀解决方案，能防御范围最为广泛的威胁，为企业提供灵活、安全的连接选项。作为思科自防御网络的核心组件，Cisco ASA 提供了主动的威胁防御，能够在攻击蔓延到整个网络之前进行阻止，控制网络活动和应用流量，并提供灵活的 VPN 连接。

Cisco ASA 自适应安全设备结合了多个协同工作的高性能处理器，以提供高级防火墙服务、IPS 服务、Anti-X/内容安全服务、IPSec 和 SSL VPN 服务等，提供了强大的应用安全性、基于用户和应用的访问控制、蠕虫与病毒防御、恶意软件防护、内容过滤以及远程用户/站点连接。同时，还可以通过安装 Cisco ASA 安全服务模块，如提供入侵防御服务的高级检测和防御安全服务模块（AIP SSM）或提供高级 Anti-X 服务的内容安全和控制安全服务模块（CSC SSM），添加更多高性能安全服务。这种灵活的设计使 Cisco ASA 能够独特地应对新威胁、在快速发展的威胁环境中提供保护，并通过可编程硬件使该平台适应未来的变化，从而实现出色的投资保护。

提示：面对 Internet 上五花八门的不同威胁，无法再简单地像以往那样有了一套防火墙就万事大吉了。对完整的防护措施而言，一个多重防护的方法必不可少。虽然 ASA 的确是一个很好的选择，但是这也并不意味着它是唯一选项。许多生产商（特别是国内安全厂商）都提供了很好的产品，因此可选择的余地还是很大的。

Cisco ASA 自适应安全设备的原有产品是 Cisco ASA 5500 系列（如图 15-10 所示），包括 Cisco ASA 5505、Cisco ASA 5510、Cisco ASA 5520、Cisco ASA 5540、Cisco ASA 5550 和 Cisco ASA 5580。最新产品则是被称为下一代防火墙服务（Next-Generation Firewall Services）的 Cisco ASA 5500-X 系列（如图 15-11 所示），包括 Cisco ASA 5512-X、Cisco ASA 5515-X、Cisco ASA 5525-X、Cisco ASA 5545-X、Cisco ASA 5555-X 和 Cisco ASA 5585-X。

图 15-10　Cisco ASA 5500 系列

图 15-11　Cisco ASA 5500-X 系列

Cisco ASA 5512-X 是一款下一代、全功能的安全设备，在一个模块化的“即插即用”设备中提供了高性能防火墙、IPSec 和 SSL VPN，以及丰富的网络服务，适用于小型企业、分支机构和大型企业远程工作人员等环境。

Cisco ASA 5515-X 在一个易于部署、经济有效的设备中为中小网络和大型企业的远程/分

支机构提供了种类丰富的高级安全和网络服务。

Cisco ASA 5525-X 凭借一个模块化、高性能的设备，为中型规模网络提供了具备主用/主用高可用性和千兆以太网连接的大量安全服务，并能随着网络安全要求的增长而扩展，从而提供了强大的投资保护功能。通过扩大 IPSec 和 SSL VPN 容量，可以支持更多的移动员工、远程地点和业务合作伙伴。Cisco ASA 5525-X 在一个集群中最多支持 10 个设备，从而每个集群能支持 SSL VPN 对或 IPSec VPN 对可以扩展 10 倍。高级应用层安全和 Anti-X 防御能通过部署 AIP SSM 的高性能入侵防御和蠕虫消除功能，或者 CSC SSM 的全面恶意软件防护而得到增强。利用可选安全环境功能，可在一个设备中部署多个虚拟防火墙，实现部门级的安全策略分区控制。这种虚拟化功能加强了安全性，降低了管理和支持总成本，同时可将多个安全设备集成到单个设备中。

Cisco ASA 5545-X 在一个可靠的模块化设备中为大中型的企业和电信运营商网络提供了具备主用/主用高可用性和千兆以太网连接的大量高性能、高密度安全服务。利用其千兆以太网接口和多达上百个 VLAN，能将网络分成多个分区，从而提高安全性。Cisco ASA 5545-X 可随着网络安全要求的提高而扩展，从而提供了强大的投资保护功能和服务可扩展性。通过部署 AIP SSM 来提供高性能入侵防御和蠕虫消除功能，提供的高级网络和应用层安全服务以及 Anti-X 防御将得到增强。同时，通过扩大 IPSec 和 SSL VPN 容量，以支持更多的移动员工、远程地点和业务合作伙伴。另外，其 VPN 集群和负载均衡功能可大幅提高 VPN 容量和永续性，并且能够十数倍提升 SSL VPN 对或 IPSec VPN 对。利用可选安全环境功能，可在一个设备中部署多达 50 个虚拟防火墙，实现部门级或每用户安全策略分区控制，同时降低管理和支持总成本。

Cisco ASA 5555-X/5585-X 在一个可靠的单机架单元设备中为大型企业和电信运营商网络提供了具备主用/主用高可用性和光纤及千兆以太网连接的大量千兆级安全服务。利用其数量众多的千兆以太网接口和 SFP 光纤接口，以及数百个 VLAN，可以将网络分成多个高性能分区，从而提高安全性。同时，还可随着企业网络安全要求的提高而扩展，从而提供了强大的投资保护功能和服务可扩展性。如图 15-12 所示为 Cisco ASA 5585-X。

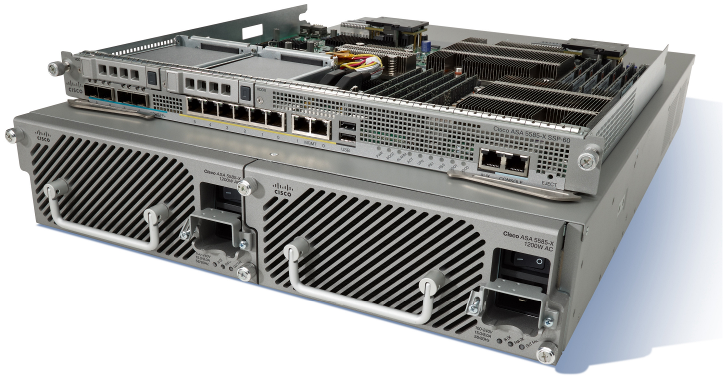


图 15-12　Cisco ASA 5585-X

表 15-4 所示为 Cisco ASA 5500 系列与 Cisco ASA 5500-X 系列性能和硬件参数比较。

表 15-4　Cisco ASA 5500 系列与 Cisco ASA 5500-X 系列比较

特　　点	Cisco ASA 5500 系列	Cisco ASA 5500-X 系列
下一代防火墙	否	是
应用可视性和控制服务	否	是
Web 安全服务	否	是
IPS 服务	是（需要单独的硬件模块）	是（不需要单独的硬件模块）
内容安全卡模块	是	类似的功能，可通过云 Web 安全（原名 ScanSafe）实现
防火墙吞吐量（最大）	-	约 4.5 倍
IPS 吞吐量（最大）	-	约 1.5 倍
VPN 吞吐量（最大）		约 1.5 倍
连接（最大）	-	约 2 倍
每秒连接数	-	约 1.5 倍
双电源	否	是
集成 I/O	-	约 2 倍
扩展 I/O	-	约 1.5 倍
CPU	单核	内核
内存	256MB～4GB	8～48GB
硬件支持 2048 位证书	否	是

15.4　IDS 与 IPS 的选择

目前，IDS 主要用于服务器群组的前端，用于侦听可能的网络攻击，为制作 IPS 和防火墙策略提供资料和素材。IPS 则往往应用于网络出口，以及所有需要被保护的位置，其正在慢慢替代防火墙，成为网络安全的新宠。

15.4.1　IDS 的选择

由于 IDS 并联于网络设备，只是侦听网络数据传输，因此，其性能对于原来的网络通信基本上没有什么影响。因此，在选择 IDS 设备时，通常只需重点考虑其所能提供的功能即可。

1.　IDS 网络检测器

网络检测器能够为网络设备及服务器上的通信模块提供全面保护。其主要特性包括以下几方面。

■　**积极响应**

系统包含对检测器设备的主动响应功能，用户只需修改 Cisco 路由器上的访问控制表（ACL）就能让系统自动回避或取消特定连接。回避功能可以临时启用，也可以长久保留。其他网络流量正常流动，只快速、有效地删除来自内部用户或外部入侵者的非法流量。这样，安全操作员就能够快速终止误操作，并防止入侵者访问网络。

■　**全面检测网络袭击**

包括检测对路由器和交换机的恶意袭击，检测面向服务器通信模块的第三层（或更低

层次）袭击、检测探听或映射等企图，例如通常作为实际袭击前兆的呼叫清除和端口清除。

■ **全面检测应用袭击**

系统支持多种应用协议，例如 HTTP、DNS、文件传输协议（FTP）及其他协议。另外，它还能检测针对易损 CGI 程序发起的多种通信袭击。

■ **预防 DoS/DDoS**

检测 Dos/DDoS 代理与黑客之间的通信，寻找知名的 DoS/DDoS 工具，例如 Trin00 和 Tribe Flood Network（TFN）。

■ **反 IDS 检测功能支持**

能够预防用于穿越典型 NIDS 技术的分组分片及其他编码技巧技术。

2. IDS 主机检测器

主机检测器能够为服务器上运行的服务器操作系统和应用提供全面保护。主机检测器安装在每台服务器上，用于保护 OS 和应用。系统利用呼叫截获技术提供纯主动式服务器安全系统，其主要特性包括以下几方面。

■ **现场预防 OS 和应用袭击**

与只有在袭击成功之后才查看记录和反应的基于记录的 HIDS 不同，主机检测器能够在袭击发生之前预防袭击。

■ **防止缓冲器溢出袭击**

主机检测器能够发现注入代码的执行过程并防止系统受损，两个主要功能如下。

- 保护与用于提供代码的手段无关，即使注入代码未通过线路传输，也能防止袭击。
- 使用了即使袭击未知也能防止执行恶意代码的通用签名的机制，对于厂商尚未提供任何补丁程序的未知缓冲器溢出，这种方法能够提供保护。

■ **不断提高完整性**

通过控制对二进制、配置数据及其他系统对象的访问，主机检测器能锁定系统。即使是超级用户，也无法篡改系统。通过配置，主机检测器可以不允许修改某些系统设置，以保证设置符合推荐的默认值。这些特性不但能强化服务器操作系统，还能显著提高系统的完整性。

■ **Web 服务器屏蔽**

为保护领先的 Web 服务器（IIS、Apache 和 I-Planet），服务器检测器包括特殊屏蔽模块。这些模块基于行为模块，能提供两种主要特性。

- 防止其他程序访问特殊应用资源（甚至在权限用户执行的时候）。
- 防止恶意使用 Web 服务器。借助 Web 服务器专用的行为模式，主机检测器能防止未知袭击，因为识别基于行为模式，且不是每次袭击都需要特殊签名。

■ **防止安全套接层（SSL）加密的 HTTP 袭击**

NIDS 不能对用 SSL 加密的 HTTP 请求进行解密。利用这个弱点，黑客可以通过对袭击加密绕过 NIDS。加密后的恶意请求能够悄悄通过 NIDS，然后由 Web 服务器解密并执行，从而成功地利用易损点。另一方面，主机检测器则与 Web 服务器相连，能够在解密服务前立即截

获请求。如果发现请求是恶意的，请求将被丢弃，而不会发送到 Web 服务器，这样就可以预防袭击。

15.4.2 IPS 的选择

由于 IPS 往往串接于网络之中，并且往往处于网络的总出口处，因此，如果 IPS 的性能较差，将会成为网络传输的瓶颈。在选择 IPS 时，除了需要考察其功能外，还应当重点考虑其处理性能。

1. IPS 的性能参数

选购 IPS 时，应当着重从以下几个方面进行考察。

■ **处理性能**

性能是 IPS 设备的基石。根据统计，国内外主流高端 IPS 产品大都采用 ASIC/FPGA/NP 的设计方案，其优点是可以提供较高的处理速度，同时具备可编程、易升级的优势。因此，主流的高端 IPS 产品大多实现了千兆位线速处理。

IPS 的处理性能大多可以从支持的用户和节点数、防火墙吞吐量、并发威胁迁移吞吐量（防火墙＋IPS 服务）、VPN 吞吐量、IPsec VPN 路数、SSL VPN 路数、并发会话路数、每秒新会话路数等参数表现出来。

为了确保高端 IPS 的带宽落到实处，一般要提供基于动态的流量控制。原因很简单，增加更多的带宽可能只会提高对非关键应用的响应速度，而不能为最需要带宽的应用提供保证，特别是对于开展大量 VoIP 应用的企业，更加需要在安全的前提下对动态流量进行分配。

■ **误报率**

误报率是 IPS 应用的核心。因为 IPS 采用 on line 模式，所以一旦出现误报，采取行动后必然会有较大影响。为此，主流的 IPS 厂商大都把精力放在降低误报率上。通常情况下，降低误报率的最好办法就是在提升性能的基础上，进行更加深入的包检测，开展更加精确的模式匹配。

■ **可用性**

由于 IPS 串接于网络之中，因此一旦 IPS 发生故障，将导致网络通信失败。对于大中型网络而言，必须考虑 IPS 的高可用性。高可用性除要求设备本身支持冗余模块和电源外，还应当支持双机备份和 by-pass 功能。当 IPS 因不堪重负而宕机时，将作为一个透明设备，网络流量将不再由 IPS 处理，而是直接通过，从而确保网络连接的畅通。

2. IPS 的功能参数

真正的 IPS 可使网络不必进行分析即可采取措施以保护系统，同时可防止攻击对操作系统、应用程序和数据造成损坏。因此，理想的 IPS 产品应当具有以下特点。

■ **主动、实时预防攻击**

真正的解决方案应该提供对攻击的实时预防和分析。IPS 应该在任何未授权活动开始前找出攻击，并防止它进入重要的服务器资源。IPS 应当集成特征检测、异常检测和拒绝服务分析技术，从而能在较大的网络流量下进行准确和智能的检测和防护，从而使企业免遭已知攻击、

首次发生的未知攻击，以及 DDoS/DoS 攻击的影响。

■ **补丁等待保护**

补丁管理是一个复杂的过程。在补丁被开发和安装期间，黑客会对服务器和重要数据进行破坏。因此，IPS 应当为网络管理员提供补丁等待期内的保护和足够的时间，以测试并安装补丁。

■ **保护每个重要的服务器**

服务器中有敏感的企业数据，是大多数黑客攻击的主要目标。所以，专门为服务器保护订制的入侵防护解决方案十分重要。因此，IPS 应当可以设定对服务器的专门保护方案，从而为企业的重要资源提供深层防护。

■ **签名和行为规则**

检测入侵最有效的方法是采取混合方式，即整合针对具体攻击的签名和行为规则的力量。这一混合方式可提供已知和未知攻击保护，而同时将误报率保持在最低，从而无需作出任何损失性让步。因此，IPS 应当以“in-line”模式配置入侵防护方案，设定响应行为，用以抓取攻击的数据包，从而在黑客对漏洞发动攻击之前，就阻止它们。

■ **深层防护**

强大的安全都是基于深度防御的概念。IPS 应当可以进行深层防护，使内部网络免遭已知攻击和首次发生的未知攻击，以及 DDos/DoS 攻击的影响。

■ **可管理性**

理想的入侵防护解决方案可使安全设置和政策被各种应用程序、用户组和代理程序利用，从而降低安装并维护大型安全产品的成本。因此，IPS 应当具有高度自动、易于管理并且拥有较高灵活性的特点，可分阶段实施安装，避免误报，使客户能够制订正确的政策，以在其独特的 IT 基础架构中阻断攻击。

■ **可扩展性**

企业级入侵防护解决方案必须可升级，以满足企业不断发展的需求，而同时保持最高水平的安全。可扩展性体现在可支持众多受保护的服务器、支持大流量和支持分散型安全管理，以满足大型分散式企业的需求。因此，IPS 应当具有良好的可扩展性，提供综合的防护体系，跨越企业核心网络、企业边界网络和分支机构的网络。

■ **动态更新**

由于 IPS 集成了庞大的攻击特征库，因此，需要由厂商长期地、不断地提供更新支持。除了可以订制 IPS 设备的过滤器之外，还应当可以通过厂商的技术支持热线，及时反馈攻击信息，以保护自身的系统。

■ **经验证的防护技术**

IPS 应当采用业界先进的新技术，经过充分测试、使用，并要持续不断地维护，只有如此，才能确保 IPS 稳定、高效地运行，并提供较高的安全性。

第 16 章　防火墙的端口与连接

防火墙只有真正连接到网络中才可以施展其强大的功能，同时防火墙位于不同的位置所发挥的作用也不尽相同。因此，不仅应当根据安全需要设计相应的拓扑结构，而且还应当根据路由器、交换机的端口类型选择彼此互连的接口。

16.1　防火墙的端口

由于防火墙往往被串连于路由器与核心层交换机之间，因此所处的网络环境相对简单，连接设备的数量也较少，端口数量较少，端口类型也相对简单。

16.1.1　防火墙物理端口

防火墙的物理端口通常只有 3 种类型，即双绞线端口、光纤端口和 SFP 插槽端口。图 16-1 所示为 Cisco ASA 5550 的内置端口和插槽。

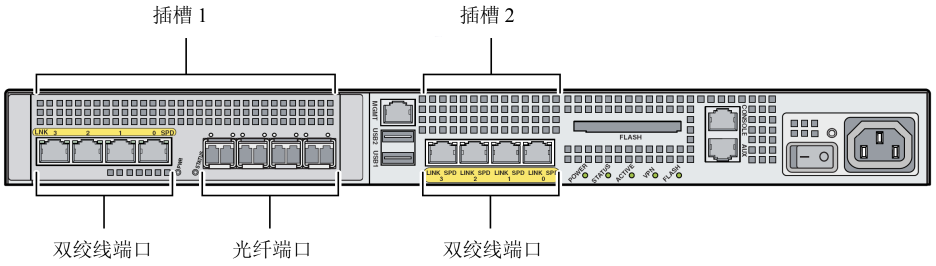


图 16-1　Cisco ASA 5550 的内置端口和插槽

当 Cisco ASA 拥有两个或以上插槽时，若欲实现数据传输的均匀分布以获得最大吞吐量，应当将安全网络和非安全网络连接至不同的插槽，从而使网络流量平均分布，并充分利用设备内置的 2 条总线。图 16-2 所示为铜缆到铜缆传输时，均匀分布流量以获得最大的吞吐量。

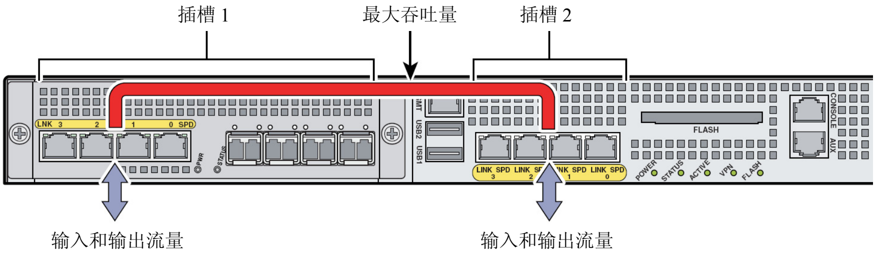


图 16-2　铜缆到铜缆的传输

图 16-3 所示为铜缆到光纤的传输，均匀分布流量以获得最大的吞吐量。

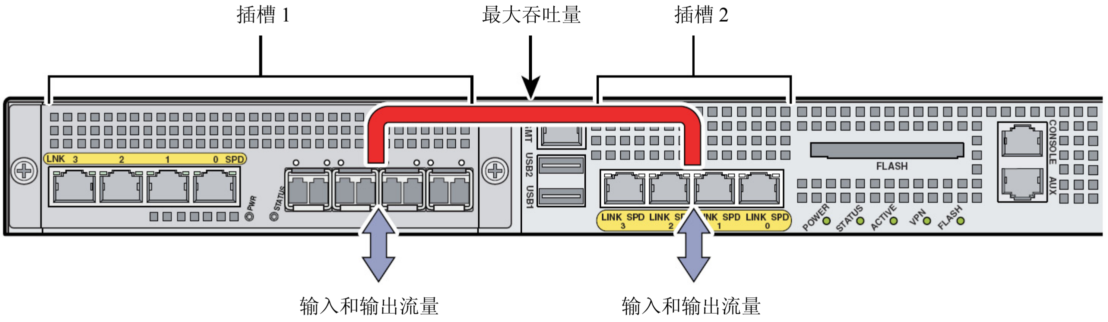


图 16-3　铜缆到光纤的传输

以下各连接方式，均只使用安全自适应设备的一个总线，因此均不能实现 IPS 数据传输的均匀分布以获得最大吞吐量。

图 16-4 所示为铜缆到的铜缆传输，由于只使用了 1 条总线，因此无法获得最大的吞吐量。

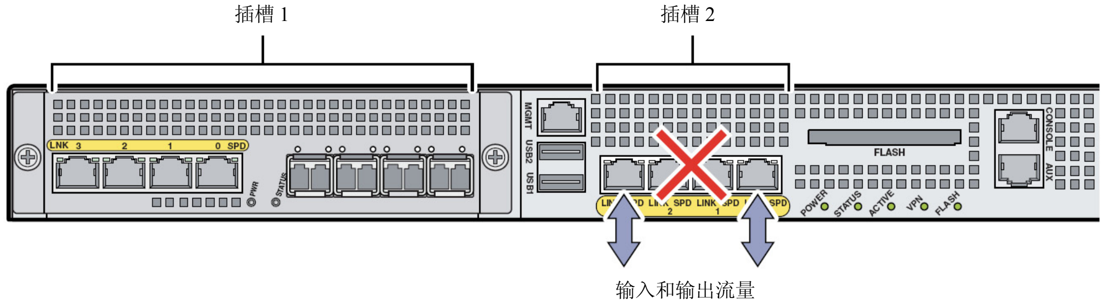


图 16-4　铜缆到铜缆的传输

图 16-5 所示为光纤到光纤的传输，由于只使用了 1 条总线，因此无法获得最大的吞吐量。

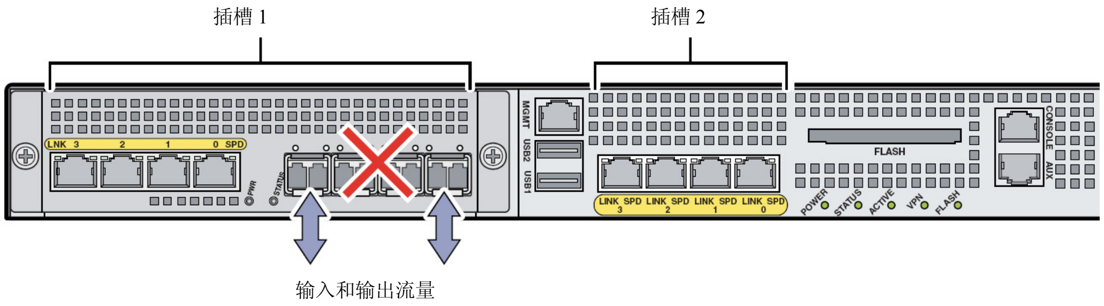


图 16-5　光纤到光纤的传输

图 16-6 所示为铜缆到铜缆的传输，同样，由于只使用了 1 条总线，因此无法获得最大的吞吐量。

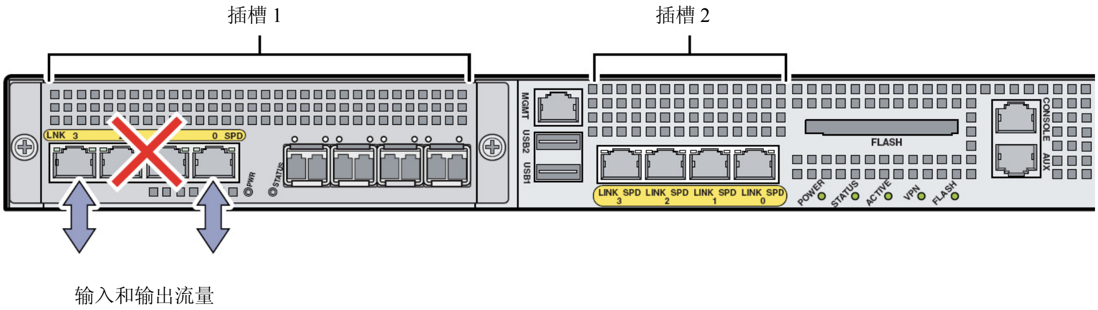


图 16-6　铜缆到铜缆的传输

图 16-7 所示为铜缆到光纤的传输，同样由于只使用了 1 条总线，因此无法获得最大的吞吐量。

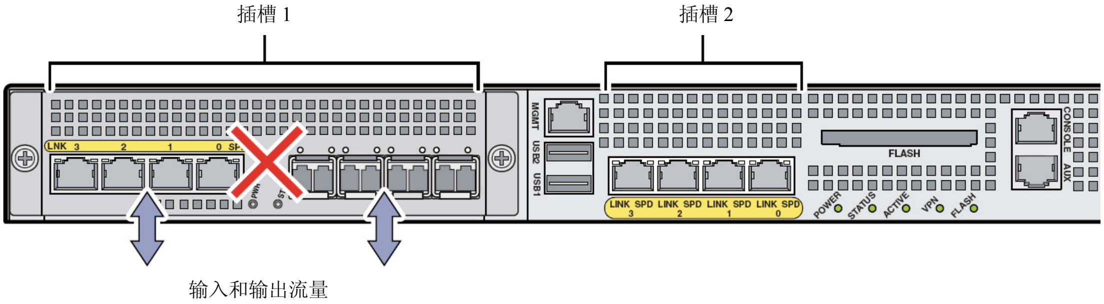


图 16-7　铜缆到光纤的传输

16.1.2 防火墙逻辑端口

防火墙端口的逻辑类型主要有 4 种，即 LAN 端口、WAN 端口、DMZ 端口和配置端口（如图 16-8 所示），分别用于连接被保护的局域网（或子网）、外网、对外发布的服务器群组，以及实现对防火墙配置的初始化。

对于 Cisco 自适应安全设备而言，由于采用模块化结构，因此，并没有给各端口直接分配端口的类型，而是在配置文件中进行指定。

图 16-8　防火墙端口类型

16.1.3 防火墙端口的连接

1. 连接 MGMT 端口

Cisco 自适应安全设备有一个专门的设备管理端口——MGMT 端口。该端口标记为 Management0/0，是一个快速以太网端口，与传统的 Console 端口类似，但 Management0/0 端

口只接收流入自适应安全设备的流量。

> **提·示**　可以使用“management-only”命令将任何端口配置为 management-only 端口，也可以在管理端口上禁用“management-only”模式。

使用双绞线跳线，将一端连接至 MGMT 端口，另外一端连接至计算机网卡，或者连接至可被网络管理的交换机，如图 16-9 所示。

2.　连接 Console/AUX 端口

Console 端口作为配置端口，需要使用 DB-9 转 RJ−45 的 Console 线，如图 16-10 所示。连接方式与路由器和交换机类似，即将 RJ−45 连接器连接至 Console 端口，另一端的 DB-9 适配器连接至计算机的串口。AUX 端口则借助 Modem 实现远程配置连接，相关内容请参见路由器连接部分。

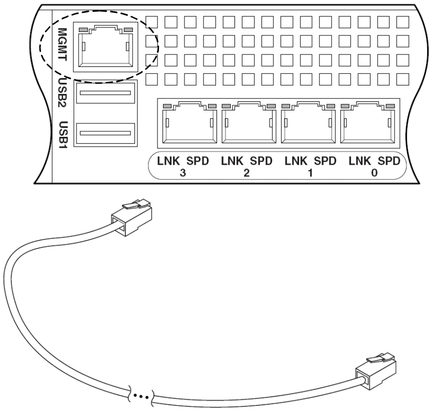


图 16-9　连接 MTMG 端口

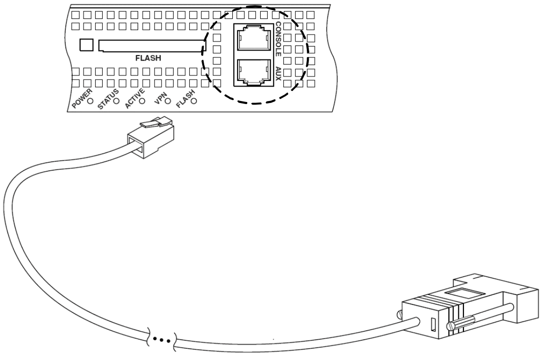


图 16-10　连接 Console/AUX 端口

3.　连接双绞线端口

使用双绞线跳线，将一端连接至 Cisco ASA 的以太网端口，另一端根据拓扑规划连接至路由器、交换机或其他网络设备，如图 16-11 所示。

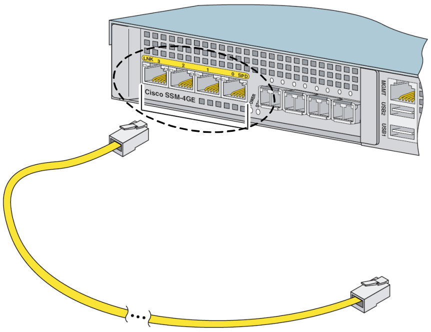


图 16-11　连接双绞线端口

4. 连接光纤端口

由于 Cisco ASA 只提供 SFP 插槽，因此在连接之前，应当先安装 SFP 模块，然后再使用 LC-LC 光纤跳线（如图 16-12 所示），根据拓扑规划将 Cisco ASA 与交换机、路由器等其他网络设备连接在一起。

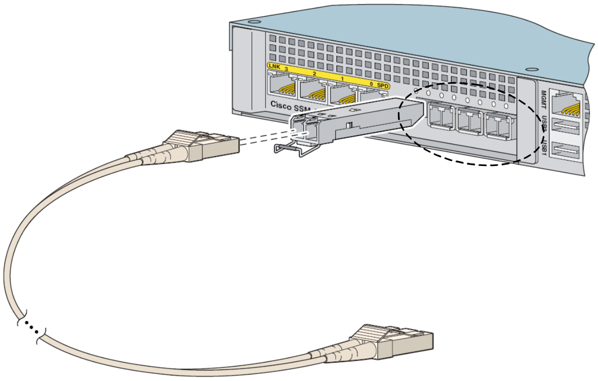


图 16-12　连接光纤端口

16.1.4 防火墙的 LED 指示灯

1. 前面板指示灯

Cisco ASA 5550 前面板 LED 指示灯（如图 16-13 所示）及其含义如表 16-1 所示。

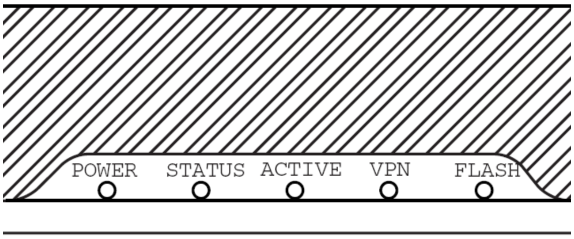


图 16-13　Cisco ASA 5550 前面板 LED 指示灯

表 16-1　Cisco ASA 5550 前面板 LED 指示灯的含义

LED	颜　色	状　态	含　义
Power	绿	亮	系统已经供电
Status	绿	闪烁	运行加电诊断或系统引导
		亮	系统加电诊断通过
	琥珀	亮	加电诊断失败
Active	绿	闪烁	网络处于活动状态
VPN	绿	亮	VPN 通道已建立
Flash	绿	亮	Flash 被访问

Cisco ASA 5545-X/5555-X 前面板及 LED 指示灯（如图 16-14 所示）及其含义如表 16-2 所示。

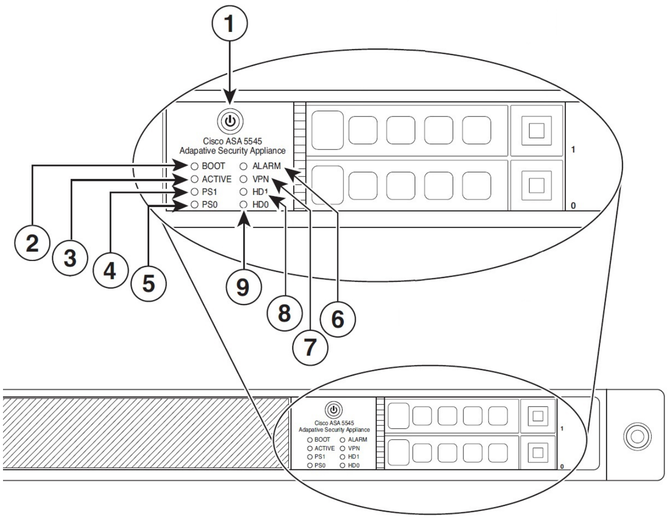


图 16-14 Cisco ASA 5545-X/5555-X 前面板及 LED 指示灯

表 16-2 Cisco ASA 5545-X/5555-X 前面板及 LED 指示灯的含义

序号	LED	描述	状态	含义
1	开关	系统软开关。按下开关时，保持在 On 状态	亮	开关处于 On 状态
			灭	开关处于 Off 状态
2	BOOT	加电诊断	闪烁绿色	加电诊断开始运行，或者系统正在引导
			固定绿色	系统已经通过加电诊断
			灭	加电诊断没有运行
3	ACTIVE	失效备援状态	固定绿色	失效备援正常运行
			灭	失效备援没有运行
4	PS1	可选冗余电源状态	亮	安装有冗余电源
			灭	未安装冗余电源
5	PS0	主电源状态	亮	主电源正常工作
			灭	主电源未正常工作
6	ALARM	系统运行状态	灭	系统运行正常
			固定琥珀色（某些设备可能是红色）	下列一个或多个严重警告： 硬件或软件严重故障 温度超过限制 电压超出允许范围
7	VPN	VPN 隧道状态	固定绿色	VPN 隧道已经建立
			灭	没有 VPN 隧道建立
8	HD1	硬盘驱动器 1 状态	闪烁绿色	硬盘正在执行读/写操作
			固定琥珀色	硬盘设备失败
			灭	没有安装硬盘
9	HD0	硬盘驱动器 0 状态	闪烁绿色	硬盘正在执行读/写操作
			固定琥珀色	硬盘设备失败
			灭	没有安装硬盘

2. 后面板和插槽端口

Cisco ASA 5550 后面板和插槽端口 LED 指示灯的含义如图 16-15 所示。

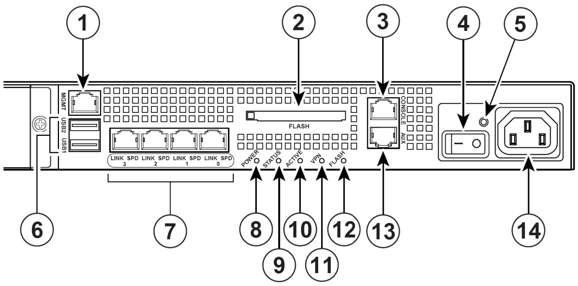


图 16-15　Cisco ASA 5550 后面板和 Slot0 插槽端口 LED 指示灯

图中：

① 管理（Management）端口。management 0/0 接口是快速以太网接口，只用于传输管理。

② 外部紧凑 Flash 插槽，为未来使用保留。

③ 串行 Console 端口。

④ 电源开关。

⑤ 电源 LED 指示灯。

⑥ USB 2.0 接口，为未来使用保留。

⑦ 网络接口，千兆位以太网接口，从左至右分别是 GigabitEthernet 0/0、GigabitEthernet 0/1、GigabitEthernet 0/2 和 GigabitEthernet 0/3。

⑧ 电源 LED 指示灯。

⑨ 状态 LED 指示灯。

⑩ 活动 LED 指示灯。

⑪ VPN LED 指示灯。

⑫ Flash LED 指示灯。

⑬ AUX 端口。

⑭ 电源连接器。

如图 16-16 所示为 Cisco ASA 5550 的 MGMT 端口和网络端口。

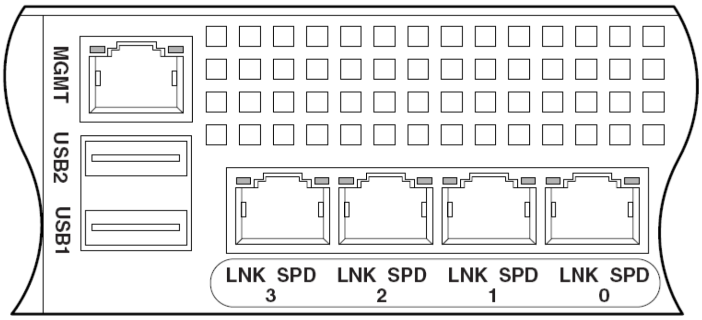


图 16-16　MGMT 端口和网络端口

Cisco ASA 5550 的 MGMT 端口和网络端口的 LED 指示灯及其含义如表 16-3 所示。

表 16-3　MGMT 端口和网络端口的 LED 指示灯的含义

指　示　灯	颜　　色	含　　义
左侧	绿色	物理连接正常
	绿色闪烁	网络活动
右侧	不亮	10 Mbps
	绿色	100 Mbps
	琥珀色	1000 Mbps

图 16-17 所示为 Cisco ASA 5550 插槽中的网络接口与 LED 指示灯。

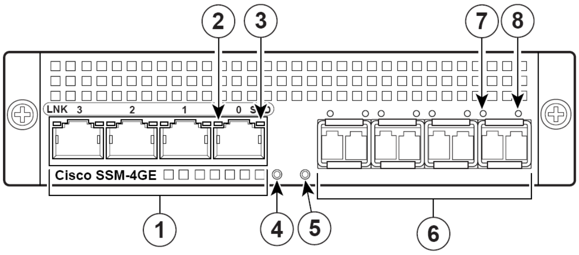


图 16-17　插槽网络接口与 LED 指示灯

图中：

① 双绞线网络端口。

② RJ-45 连接 LED 指示灯。

③ RJ-45 速率 LED 指示灯。

④ 电源 LED 指示灯。

⑤ 状态 LED 指示灯。

⑥ 光纤网络端口。

⑦ SFP 连接 LED 指示灯。

⑧ SFP 速率 LED 指示灯。

Cisco ASA 5550 插槽中的网络接口的 LED 指示灯及其含义如表 16-4 所示。

表 16-4　插槽中的网络接口的 LED 指示灯的含义

LED	颜　色	状　态	含　义
RJ-45 和 SFP 连接 LED	绿	亮	网络连接
		闪	网络活动
RJ-45 和 SFP 速率 LED	不亮	10 MB	网络未活动
	绿	100 MB	100 Mbps 网络
	琥珀	1000 MB	1000 Mbps 网络
电源 LED	绿	开	系统电源打开
状态 LED	绿	闪烁	系统正在引导
	绿	亮	系统引导正确
	琥珀	亮	系统引导失败

图 16-18 所示为 Cisco ASA 5500-X 系列后面板的 LED 指示灯。

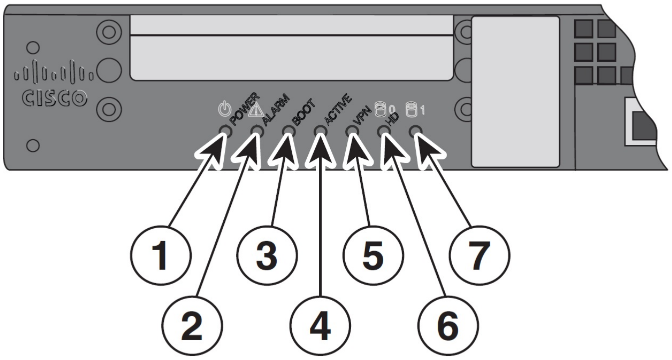


图 16-18 Cisco ASA 5500-X 系列后面板 LED 指示灯

Cisco ASA 5500-X 系列后面板的 LED 指示灯与前面板基本相同，及其含义请参见“表 16-2 Cisco ASA 5545-X/5555-X 前面板及 LED 指示灯的含义”。

图 16-19 所示为 Cisco ASA 5545-X/5555-X 系列后面板端口。

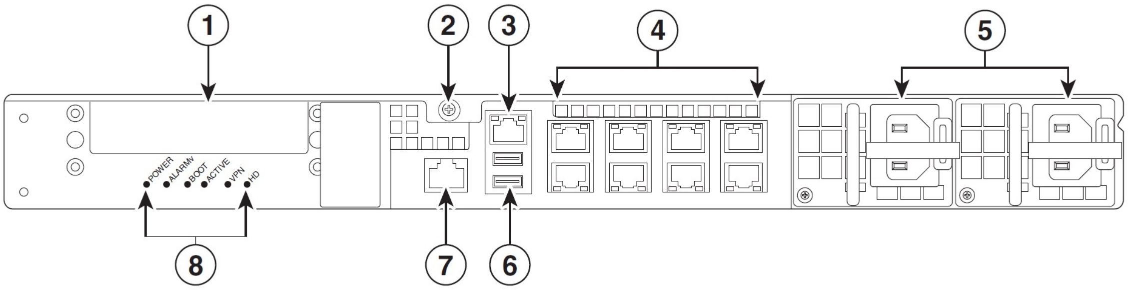


图 16-19 Cisco ASA 5545-X/5555-X 系列后面板端口

图中：

① I/O 插槽。可选 I/O 卡插槽，如果安装有光纤 I/O 卡，应当使用 SFP 模块连接。

② 接地螺钉。

③ Management 0/0 端口。该千兆以太网接口仅用于管理连接。使用 RJ-45 线缆。

④ RJ-45 端口。千兆以太网数据接口，上排从左至右为 7、5、3、1，下排从左至右为 6、4、2、0。

⑤ 电源线接口。

⑥ USB 端口。2 个 USB 标准接口。

⑦ Console 端口。使用 Console 线直接连接至管理计算机。

⑧ 后面板 LED 指示灯。

16.2 防火墙的应用环境与连接

在每一种网络环境下防火墙的安装位置和连接方式可能都不相同。传统的做法就是将防火墙安装在内部机构网络与外部网络之间，至于内部网络之间可能还需要设置安全隔离措施，也同样可以安装防火墙。

16.2.1 防火墙连接策略

在设有网络防火墙的网络中，信息只能够按照防火墙图标箭头指向的一方传输，而反方向传来的数据则会被防火墙拦截，为防火墙的不信任区域。例如，在如图 16-20 所示的网络结构中，网络 D 对所有网络都是不信任的，即其他网络发送过来的所有文件都要经过拦截；网络 A 对网络 D 和网络 C 是信任的，而对网络 B 是不信任的；网络 C 信任网络 D 而不信任网络 A；网络 B 信任连接到它的所有网络。

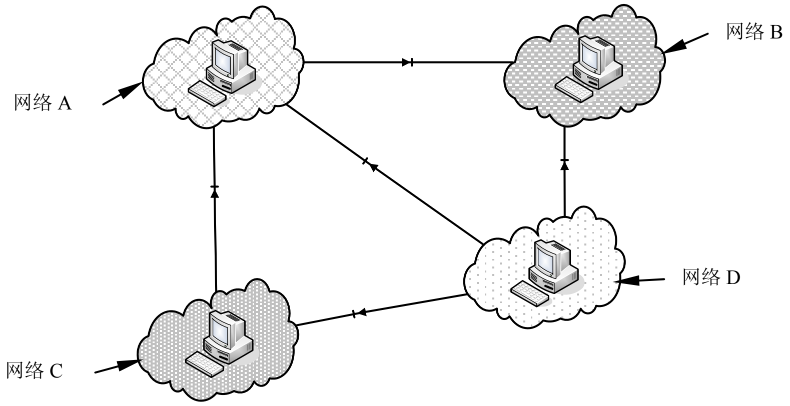


图 16-20　各个网络边界的防火墙

如今许多用户接入 Internet 的方式都是局域网共享接入，因此相对而言防火墙的不信任区域就是广域网，利用路由器来实现内部网络和广域网的互连，路由器所在的位置也应当是防火墙的位置，许多路由器产品也集成了防火墙的功能。

当防火墙拥有两个端口时，其中一个端口用来连接路由器，另一个端口用来连接内部网络，如图 16-21 所示。

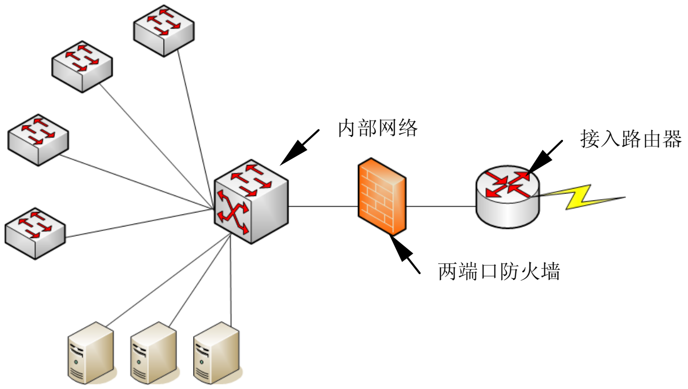


图 16-21　两个端口的防火墙连接

当防火墙只提供一个连接端口时，一般采用如图 16-22 所示的连接方式，即将防火墙直接连接至工作组交换机上即可。

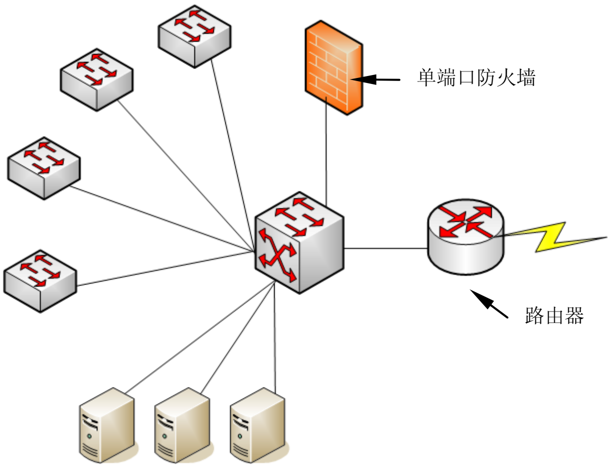


图 16-22　单端口防火墙连接

16.2.2 内部网络与 Internet 之间的连接

这是一种应用最广，也是最重要的防火墙应用环境。在这种应用环境下，防火墙主要保护内部网络不受非法用户的攻击。目前绝大多数企业网络安装防火墙的主要目的就在于此。在这种应用环境中，一般情况下防火墙网络可划分为表 16-5 中的 3 个不同级别的安全区域，如图 16-23 所示。

表 16-5　连接内外网防火墙的不同安全区

内部网络	这是防火墙要保护的对象，包括全部的企业内部网络设备及用户主机，这个区域是防火墙的可信区域（这是由传统防火墙的设计理念决定的）
外部网络	这是防火墙要防护的对象，包括外部 Internet 主机和设备，这个区域为防火墙的不可信任网络区域（也是由传统防火墙的设计理念决定的）
DMZ（Demilitarized Zone，非军事区）	它是从企业内部网络中划分的一个小区域，在其中就包括内部网络中用于公众服务的外部服务器，如 Web 服务器、邮件服务器、FTP 服务器、外部 DNS 服务器等，它们都是为 Internet 提供某种信息服务

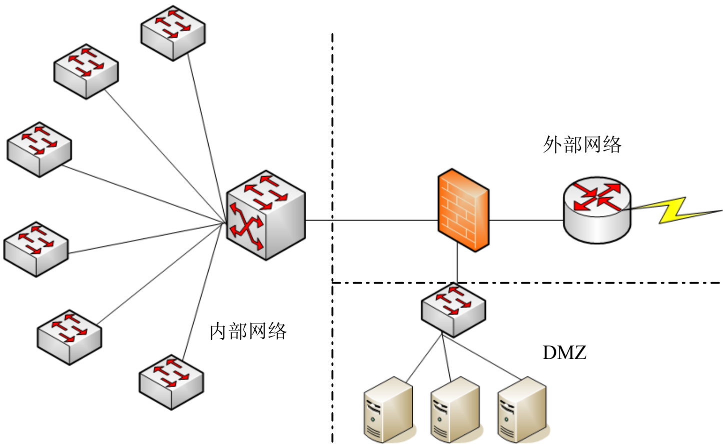


图 16-23　防火墙分割的 3 个区域

在这3个区域中，用户需要对不同的安全区域设置不同的安全策略。虽然内部网络和DMZ都属于企业内部网络的一部分，但它们的安全级别（策略）是不同的。对于要保护的大部分内部网络，一般情况下禁止所有来自因特网用户的访问；而由企业内部网络划分出去的DMZ，因需为因特网应用提供相关的服务，所以在一定程度上，没有内部网络限制那么严格，如Web服务器通常是允许任何人进行正常的访问。那么，这些服务器是不是很容易被攻击呢？由于在这些服务器上所安装的服务非常少，所允许的权限非常低，真正的服务器数据保证在受保护的内部网络主机上，所以黑客攻击这些服务器没有任何意义，既不能获取什么有用的信息，也不能通过攻击它而获得过高的网络访问权限。

提·示 建议通过NAT（网络地址转换）技术将受保护的内部网络的全部主机地址映射成防火墙上设置的少数几个有效公网IP地址。这样有两个好处：一则可以对外屏蔽内部网络构和IP地址，保护内部网络的安全；同时因为是公网IP地址共享，所以可以大大节省公网IP地址的使用，节省了企业投资成本。

16.2.3 连接局域网和广域网

局域网和广域网之间的连接是应用防火墙最多的网络，不过网络用户可根据自己具体需要的不同面订制不同的连接。

如果用户网络原来已存在边界路由器，则可充分利用原有设备，利用边界路由器的包过滤功能，添加相应的防火墙配置，这样原来的路由器也就具有防火墙功能了。然后再利用防火墙与需要保护的内部网络连接。对于DMZ中的公用服务器，则可直接与边界路由器相连，不用经过防火墙。它可只经过路由器的简单防护。在这种网络环境中，边界路由器与防火墙就一起组成了两道安全防线（如图16-24所示），并且在这两者之间可以设置一个DMZ，用来放置那些允许外部用户访问的公用服务器设施。

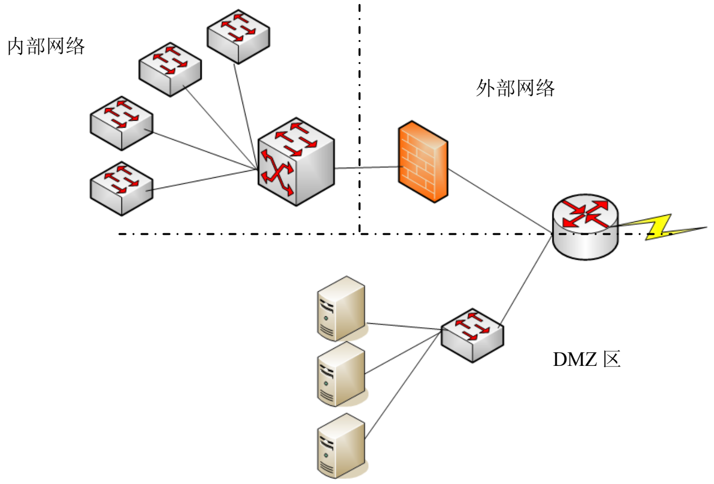


图16-24 存在边界路由器网络连接

如果用户网络中不存在边界路由器，则此时直接由防火墙来保护内部网络（如图16-25所

示）。此时 DMZ 区域和需要保护的内部网络分别连接防火墙的不同 LAN 网络接口，因此需要对这两部分网络设置不同的安全策略。这种网络中虽然只有一道安全防线，但对于大多数中、小企业来说是完全足够的。不过在选购防火墙时就要注意，防火墙一定要有两个以上的 LAN 网络接口。

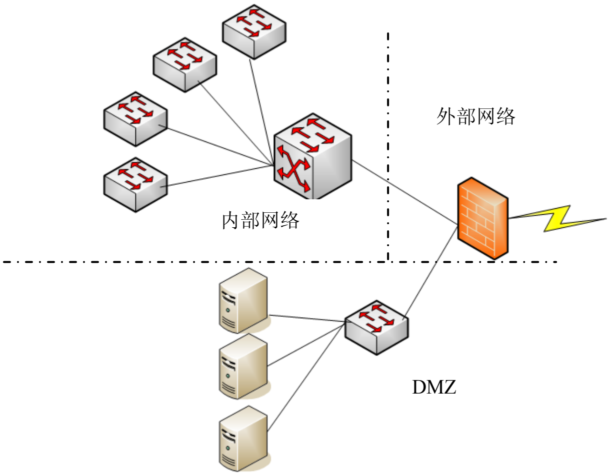


图 16-25　无边界路由器的网络连接

16.2.4 内部网络与第三方网络之间的连接

这种应用主要是针对一些规模比较大的企业用户，它们的企业内部网络通常要与分支机构、合作伙伴或供应商的局域网进行连接，或者是同一企业网络中存在多个子网。在这种应用环境下，防火墙主要限制第三方网络（如合作伙伴等）对内部网络的非法访问，如图 16-26 所示。在这种网络环境中通常是将安全性要求较低的服务器直接连接在网络防火墙的 LAN 端口上，通过防火墙对这些服务器做一些简单的配置，可以提供第三方网络所需的功能即可。

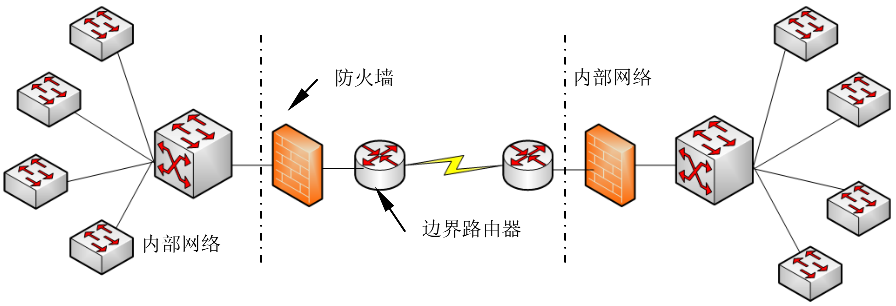


图 16-26　连接内部网络和第三方网络

在这种防火墙应用网络环境中，根据企业是否需要 DMZ（放置一些供第三方网络用户访问的服务器），又可以分为两种具体的网络环境。

1.　需要 DMZ

这种情况是企业需要为第三方网络提供一些公用服务器，供日常访问。这种网络环境与

上面所介绍的限制因特网用户非法访问企业内部网络一样，整个网络同样可分为 3 个区域，如表 16-6 所示。

表 16-6　连接内网和第三方网络的防火墙安全区划分

内部网络	这是防火墙要保护的对象，包括全部企业内部网络中需要保护的设备和用户主机，是防火墙的可信任网络区域，区域中的所有用户看不到第三方网络的存在
外部网络	防火墙要限制访问的对象，包括第三方网络主机和设备，是防火墙的不可信任网络区域
DMZ	由企业内部网络中一些外部服务器组成，包括公众 Web 服务器、邮件服务器、FTP 服务器、外部 DNS 服务器等。这些公众服务器为第三方网络提供相应的网络信息服务

需要保护的内部网络和 DMZ 的安全策略也是不同的：需要保护的内部网络一般禁止来自第三方的访问，而 DMZ 则是为第三方提供相关的服务，允许第三方的访问。

2.　不设置 DMZ

在这种网络环境中只包括内部网络和外部网络两个区域。某些需要向第三方网络提供特殊服务的服务器或主机与需要保护的内部网络通过防火墙的同一 LAN 端口连接，作为内部网络的一部分，只是通过防火墙配置对第三方开放内部网络中特定的服务器/主机资源。但要注意的是，这种配置可能带来极大的安全隐患，因为来自第三方网络中的攻击者可能破坏和控制对他们开放的内部服务器/主机，并以此为据点，进而破坏和攻击内部网络中的其他主机/服务器等网络资源。

16.2.5 内部网络不同部门之间的连接

这种应用环境就是在一个企业内部网络之间，对一些安全性要求较高的部门（如人事管理、财务管理等）进行隔离保护。通过防火墙保护内部网络中敏感部门的资源不被非法访问。在这些部门网络主机中的数据对于企业来说是非常重要的，它的工作不能完全离开企业网络，但其中的数据又不能随便供网络用户访问。这时有几种解决方案，通常是采用 VLAN 配置，但这种方法需要配置三层以上的交换机，同时配置方法较为复杂。另一种有效的方法就是采用防火墙进行隔离，在防火墙上进行相关的配置（比起划分 VLAN 来简单许多）。通过防火墙隔离后，尽管同属于一个内部局域网，但是其他用户的访问都需要经过防火墙的过滤，符合条件的用户才能访问。这类防火墙通常不仅通过包过滤来筛选数据包，而且还要对用户身份的合法性（在防火墙中可以设置允许哪此些用户访问）进行识别。通常为自适应代理服务器型防火墙，这种防火墙方案还可以有日志记录功能，对网管员了解网络安全现状及改进非常重要。

16.2.6 连接同一部门的不同网络

这种连接方式在安全性要求较高的企业网络中比较常见，例如跨国公司等，公司内部网络包含多个部门的子网络，而有些局域网的数据是不允许其他用户随意访问的，因此，就要在这些局域网中设置防火墙进行隔离。在如图 16-27 所示的网络中，同是一个企业的内部网络，可以将需要受到保护的重要部门和一些服务器通过防火墙连接至其他网络。

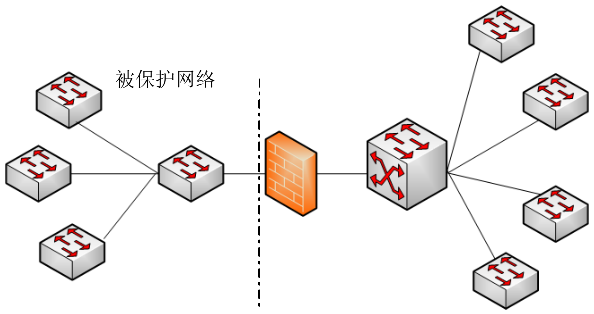


图 16-27　连接内部子网络

16.2.7 用户与中心服务器之间的连接

对于一个服务器中心而言，大多服务器都需要对第三方（合作伙伴、因特网用户等）开放，但是所有这些服务器分别属于不同用户所有，其安全策略也各不相同。如果把它们都定义在同一个安全区域中，显然不能满足各用户的不同需求，这时就可以按不同安全策略保护这些服务器。根据实施方式的不同又可以分为以下两种网络环境。

- 每台服务器单独配置独立的防火墙

这种方法是最容易实现的也是最直观的，但这种方案无论从经济上、还是从使用和管理的灵活可靠性上都不是最好的。一则需要购买与托管服务器数据一样多的防火墙，对托管中心来说投资非常大；而且托管中心管理员面对这么多防火墙，其管理难度可想而知。

- 配置虚拟网络防火墙

这主要是利用三层交换机的 VLAN 功能，先在三层交换机上将有不同安全要求的服务器划分至不同的 VLAN，然后借助对高性能防火墙模块的 VLAN 子网配置，将防火墙划分为多个虚拟防火墙（如图 16-28 所示）。这种方案虽然配置较为复杂，但一旦配置完成，随后的使用和管理将相当方便，就像用交换机管理多个 VLAN 子网一样来管理每个用户服务器，而且该方案在现实中比较经济可行。

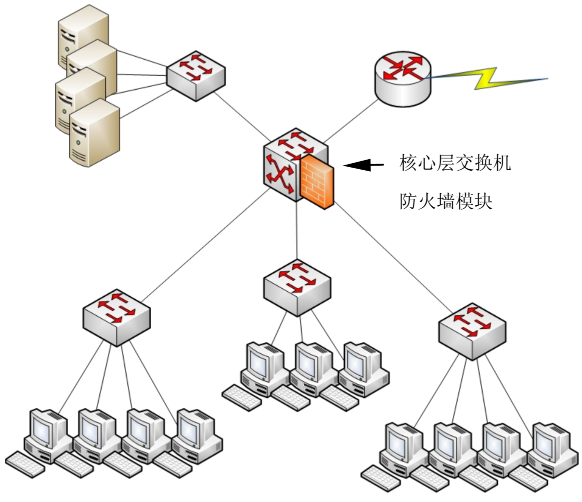


图 16-28　虚拟防火墙

提・示 借助三层交换机或路由器内置的防火墙模块，也可以为不同的用户 VLAN 配置不同的安全策略，从而将网络攻击限制在不同的 VLAN 中，进而保证整个网络的安全。

16.3　IPS 的网络应用与连接

IPS 与防火墙在网络中的连接方式基本相似，不过，也有其较为特殊的方式。通常情况下，依据 IPS 防护的区域不同，而将其连接至不同的位置。

16.3.1 路由防护

路由防护，将 IPS 直接部署至路由器和核心层交换机之间，借助网络的边界防护，实现 IPS 和防火墙功能，为整个网络提供网络安全保护，如图 16-29 所示。

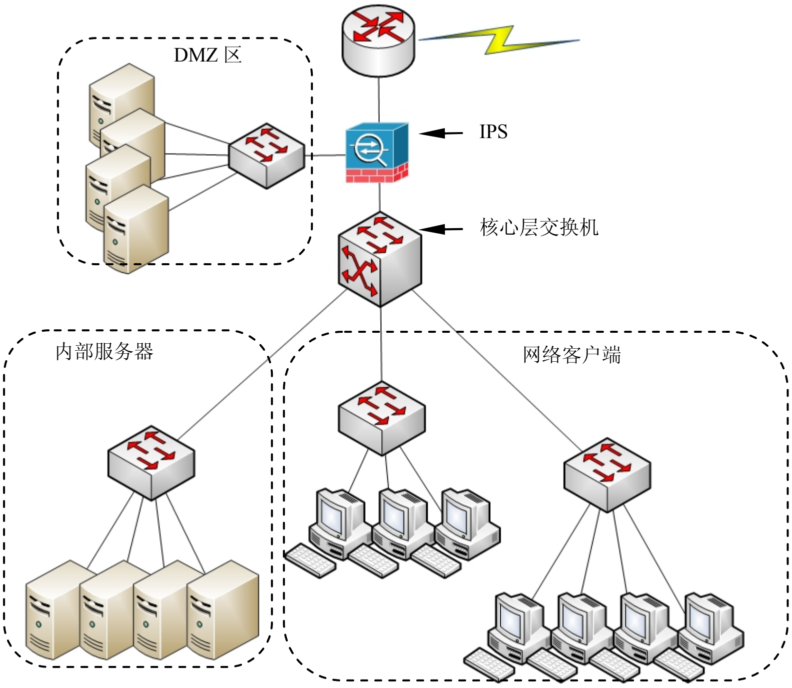


图 16-29　路由防护

16.3.2 交换防护

将 IPS 作为网络核心，采用一进多出或多进多出的方式，实现不同网段相互连接，进行数据交换，同时实现防火墙功能，如图 16-30 所示。

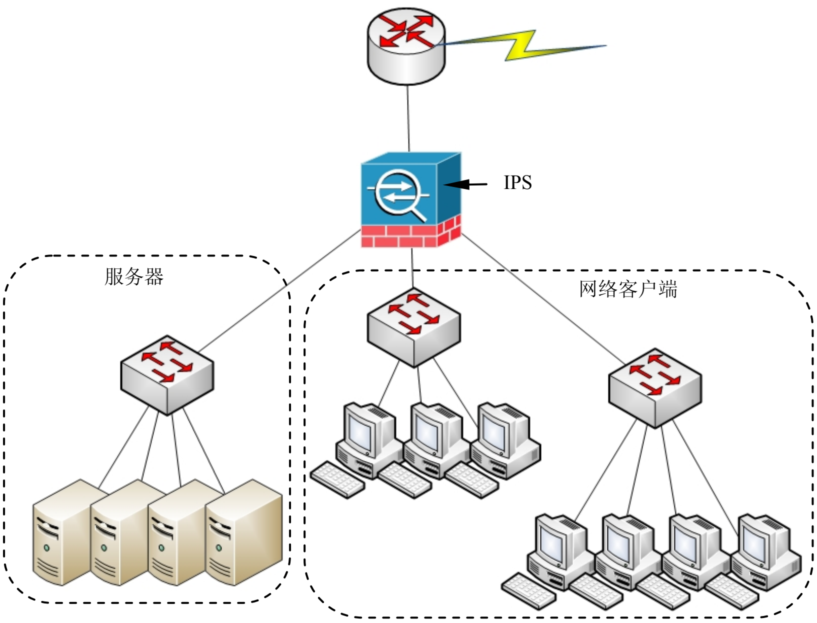


图 16-30　交换防护

16.3.3 多链路防护

采用多路 IPS 的连接方式，一路 IPS 防护一个 ISP 接入，各路 IPS 相互独立，彼此之间没有数据交换，互不干扰，如图 16-31 所示。

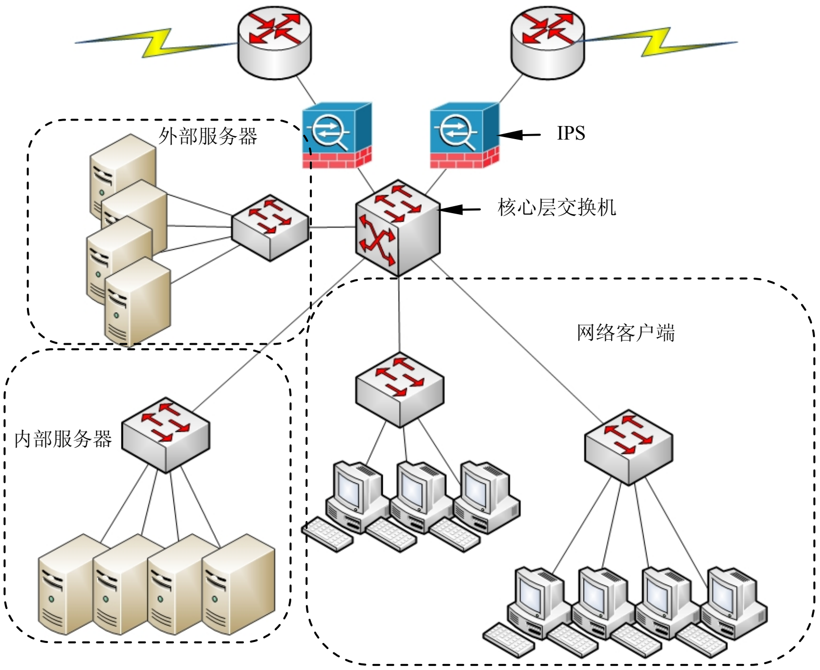


图 16-31　多链路防护

16.3.4 混合防护

多种模式分层防护，监控与防护相结合，更加完善。在线 NIPS 模式、旁路 NIDS 模式相配合，如图 16-32 所示。

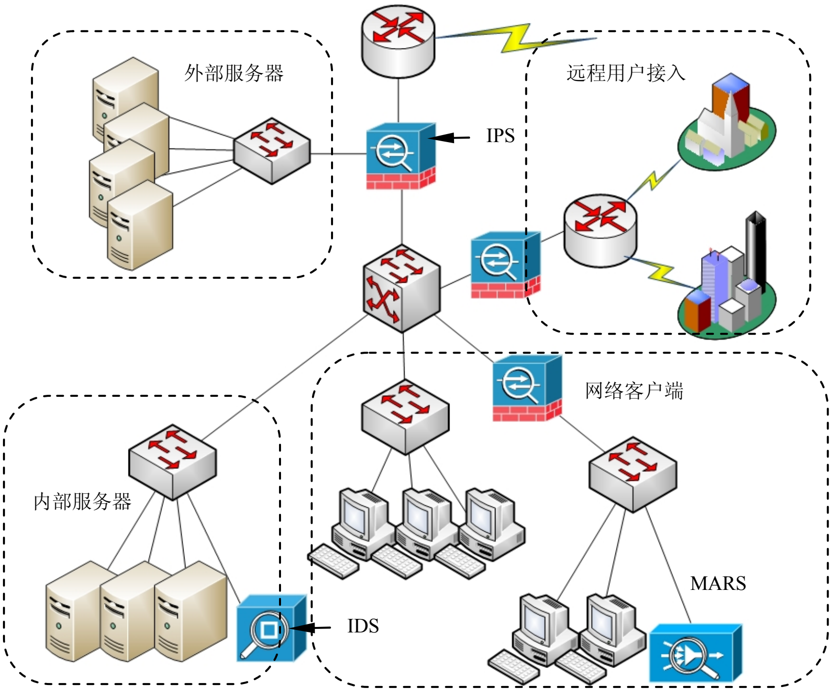


图 16-32 混和防护

第 17 章　使用 ASDM 配置管理防火墙

只要允许外部网络上的计算机直接访问内部网络上的计算机，就存在着攻击者可以损害内部局域网上计算机的安全性问题，并从那里攻击其他计算机的可能性。为了保证内部网的安全，防止非法入侵，需要配置并使用专用的网络防火墙。

17.1　Cisco ASDM 初始化与访问

Cisco 自适应安全设备管理器（Adaptive Security Device Manager，ASDM）通过一个直观、易用、基于 Web 的管理界面，提供了世界级的安全管理和监控服务。结合 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备，Cisco ASDM 提供的智能向导、强大的管理工具和灵活的监控服务，进一步增强了 Cisco 安全设备套件提供的先进的集成安全和网络功能，从而加速安全设备的部署。其基于 Web 的安全设计可使用户能随时随地访问 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备。

17.1.1　Cisco ASDM 简介

作为自适应安全设备管理器，Cisco ASDM（如图 17-1 所示）以图形界面方式，配置和管理 Cisco ASA 和 Cisco PIX 安全设备。

图 17-1　Cisco ASDM

Cisco ASDM 具有如下特点。

1. 集成化管理提高管理效率

网络上任何支持 Java 插件的计算机，都可以借助 Web 浏览器访问 Cisco ASDM，使安全管理员能迅速、安全地访问自己的 Cisco ASA 和 Cisco PIX 设备。为管理员提供了基于 Windows 的全新配置方式，管理员可从单一管理工作站连接至多个安全设备，从而提高了配置和管理安全设备的效率。

2. 启动向导加速安全设备的部署

Cisco ASDM 拥有一个启动向导，加速了安全设备部署流程。一系列简单的渐进式配置界面，可帮助管理员快速启动和运行设备，创建使流量能安全地在网络中传输的稳固配置。该启动向导能配置多种可选特性，如动态主机控制协议（DHCP）服务器设置、网络地址转换（NAT）、管理员访问和自动更新。自动更新是一个具革命性意义的远程管理功能，可确保设备配置和软件镜像保持最新状态。除此之外，还拥有 VPN 向导、高可用性和扩展性向导、统一通信向导、包捕捉向导，可以在向导指引下完成各种重要配置和监控（如图 17-2 所示）。

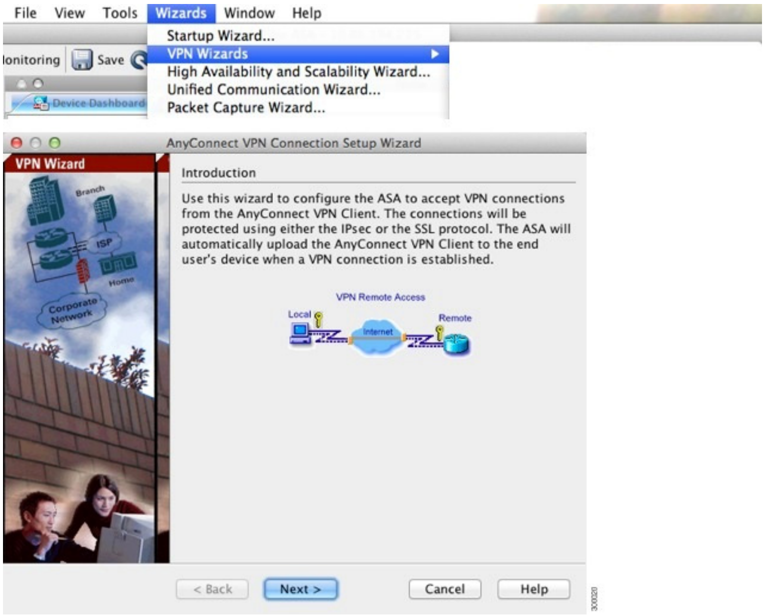


图 17-2　Cisco ASDM 向导

3. 仪表盘提供重要实时系统状态信息

Cisco ASDM 拥有一个动态仪表盘，提供全面的系统概述和设备状态统计数据概览（如图 17-3 所示）。可自动检测所配置的 Cisco 安全设备，并显示每个设备的软件版本、许可信息和重要统计数据。在复杂的网络环境中，不仅为管理员提供了实时状态指示灯，还为强大的分析工具和高级监控功能提供了启动点。其实时系统日志浏览器，具有模式匹配功能，可根据网络地址、端口号、主机名等过滤系统日志。此外，还提供了一个强大的搜索引擎，可帮助管理员确定在何处配置特定特性，只需点击鼠标即可方便地获得搜索结果。

图 17-3　Cisco ASDM 仪表盘

4.　安全策略管理降低运营成本

Cisco ASDM 强大的管理服务功能，简化了安全策略定义和持续策略维护，使安全管理员能创建可重复使用的网络和服务对象组，以及可实施多项安全策略的策略检测图（如图 17-4 所示）。支持范围广泛的访问控制功能，如基于用户和用户组的访问列表、基于时间的访问列表，以及进/出访问列表。管理员可根据不同条件划分网络流或流量级别，然后向每个流或流量级别应用一套可订制的检测服务、服务质量（QoS）服务和连接服务。这些先进的访问控制和应用检测功能，与易用的持续策略管理服务相配合，可确保各种规模的企业都能获得强大、动态的安全设置。

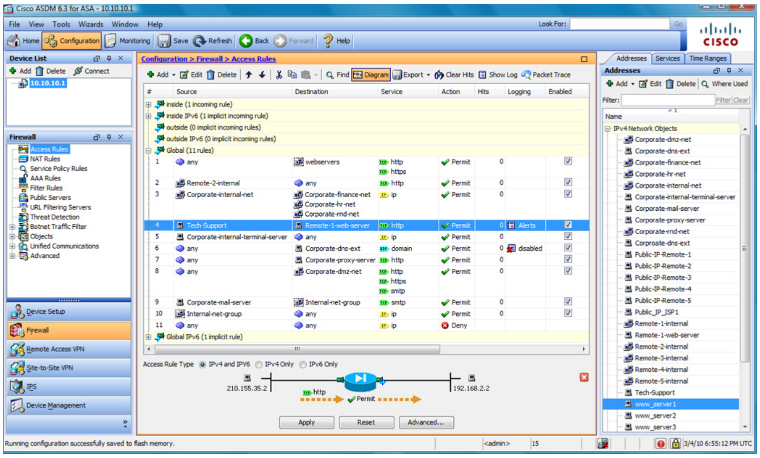


图 17-4　Cisco ASDM 访问策略

5.　安全服务实现基于角色的安全访问

Cisco ASDM 集成了一系列强大的安全服务，可防止对设备进行未授权管理访问。支持多种验证管理员的方法，如 Cisco ASA 或 Cisco PIX 的本地验证数据库，或者由 RADIUS/TACACS 服务器进行验证。Cisco ASDM（运行在管理员计算机上）和安全设备间的所有通信，都通过采用 56 位数据加密标准（DES），或者更安全的 168 位三重 DES（3DES）算法的安全套接字

层（SSL）加密。Cisco ASDM 支持多达 16 级可订制管理访问级别，为管理员和操作人员提供相应的许可级别，来访问所管理的每个 Cisco 安全设备（如仅限监控、只读访问配置等）。

6. VPN 管理将安全连接扩展到远程站点

Cisco ASDM 具有全面的 VPN 配置功能，借助简化配置的智能 VPN 向导（如图 17-5 所示），帮助企业为站点间 VPN 部署而建立因特网密钥交换（IKE）和 IP 安全（IPSec）策略。Cisco ASDM 还为 Cisco Easy VPN 远程接入 VPN 集中器服务提供了丰富的管理功能，支持 VPN 客户端安全状态增强、自动软件升级、VPN 集群等特性。在 Cisco ASA 5500-X/5500 系列上，Cisco ASDM 集成了全面的 Cisco WebVPN 管理特性，使管理员能快速配置和支持 Web 浏览器发出的远程接入连接，及其本地 SSL 加密。Cisco ASDM 也提供了先进的 VPN 监控功能，为管理员提供了大量的统计信息和图形，显示进程正常运行时间、每进程传输数据等参数。

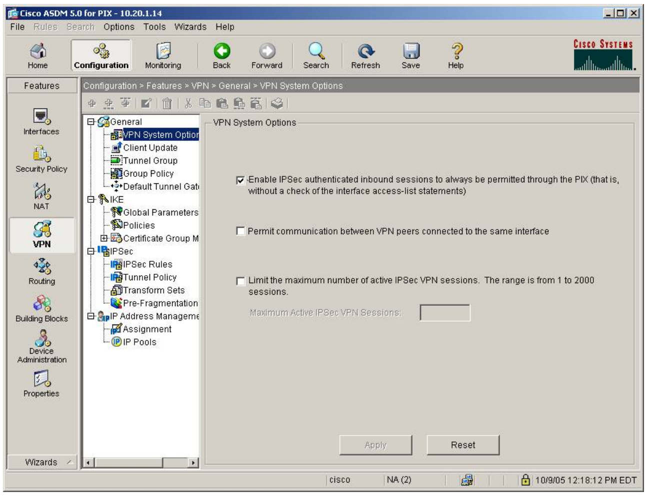


图 17-5　VPN 配置

7. 管理服务与应用检测相互协作

Cisco ASA 7.0 版及以上版本包括 30 多种专用检测引擎，用于各种采用超文本传输协议（HTTP）、文件传输协议（FTP）、GPRS 隧道协议（GTP）、Sun 远程过程调用（SunRPC）、H.323 和会话启动协议（SIP）等协议的现代应用。Cisco ASDM 支持智能应用默认设置的点击功能，可快速建立强大的安全配置，保护关键任务型应用和资源免遭误用和隧道攻击。还可对检测服务定义基于信息流的控制，并为管理员提供企业级工具来对应用进行细致的控制。

8. 智能用户界面简化网络集成

Cisco ASDM 可简单、方便地管理 Cisco ASA 和 Cisco PIX 中丰富的网络集成特性。虚拟化功能可在单一安全设备中创建多个安全环境（虚拟防火墙），每个环境有自己的安全策略、逻辑接口和管理域。Cisco ASDM 采用一个智能虚拟化管理系统，为需要全面了解系统中所有虚拟防火墙和特性的中央系统管理员提供了无限制的访问。各环境的用户都能获得相同的 Cisco ASDM 的界面和外观，以及同样丰富的管理和监控功能，但所访问的配置和特性仅限于中央系统管理员为其分配的环境。各环境用户可在管理员创建的安全策略基础上，使用 Cisco

ASDM 为其虚拟防火墙建立订制配置。

Cisco ASDM 使管理员能全面控制组播路由协议，如协议无依赖型组播（PIM）协议、最短路径优先（OSPF）动态路由协议（如图 17-6 所示）、基于 IEEE 802.1q 的 VLAN 接口和服务质量（QoS）机制。对于新用户，它将智能默认设置和详细的在线帮助相结合，可简化这些网络服务的配置。高级用户则可利用深层特性支持，将 Cisco 安全设备集成入复杂的路由和交换环境中。

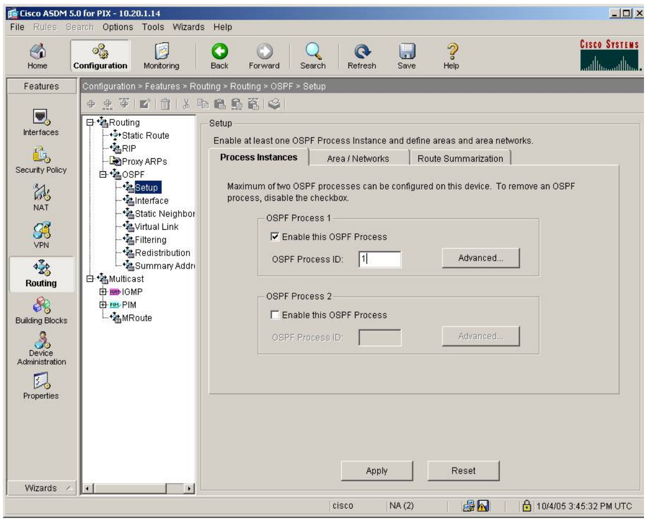


图 17-6　高级 OSPF 配置

9.　安全管理界面提供一致的管理服务

Cisco ASDM 为 Cisco ASA 的所有配置、管理和监控需求提供了一致的解决方案。除了可提供最佳安全和 VPN 服务的丰富的配置和管理选项外，它还提供了一个企业级解决方案，来管理 Cisco ASA 5500/5500-X 系列真正的自适应安全服务。

Cisco ASDM 可帮助企业提高其网络环境的安全级别，通过 Cisco 高级检测和保护安全服务模块（AIP-SSM）简化对各种防御的管理，从而降低运营成本。这些服务提供了针对入侵、网络攻击、拒绝服务（DoS）攻击，以及蠕虫、网络病毒、特洛伊木马、间谍件和广告件等恶意件的防御。Cisco ASDM 使管理员可迅速配置这些服务，包括流量风险评估和元事件生成器等独特的 Cisco 准确防御技术。Cisco ASDM 使企业能更为自信地保护网络免遭各种攻击，而且不会有丢弃合法网络流量的风险。

10.　监控和报告工具实现关键业务数据分析

■　监控工具

Cisco ASDM 在主页上提供了深入的监控和报告服务，以及概览监控功能（如图 17-7 所示）。灵活的分析工具能够创建图形化总结报告，显示实时使用率、安全事件和网络活动。每个图形化报告中的数据都能以订制增量的形式提供，用户可选择 10 s 快照或进行更长时间间隔的分析。同时浏览多个图的能力使用户可并行执行具体评估。各图形能方便地标记，并输出数据以便以后访问。

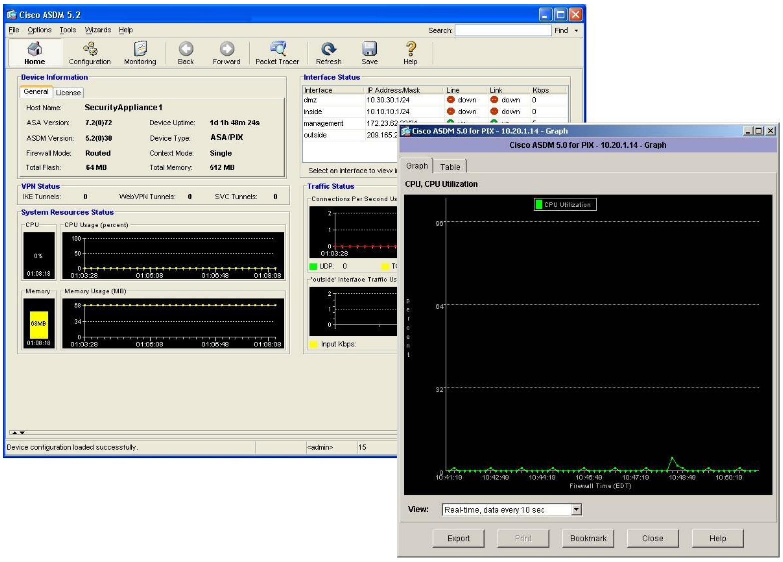


图 17-7　监控窗口

■　**系统图**

提供 Cisco ASA 5500/5500-X 系列自适应安全设备的具体状态信息，包括所用区块和空闲区块、当前内存利用率和 CPU 利用率。

■　**连接图**

跟踪实时进程和连接性能监控数据；地址转换；验证、授权和记账（AAA）事务处理；URL 过滤请求等。连接图使管理员可全面了解其网络连接和活动，且不会被过多信息所淹没。

■　**攻击保护系统图**

有 16 种不同的图形来显示潜在的恶意活动。攻击特征信息显示 IP、因特网控制信息协议（ICMP）、用户数据报协议（UDP）、TCP 攻击和 Portmap 请求等活动。这些图形也详细显示了攻击者列表、事件列表、系统统计数据和对于 Cisco AIP-SSM 的诊断。

■　**接口图**

提供对安全设备上每个接口的带宽使用率的实时监控。显示内外通信的带宽使用率。用户可浏览分组速率、数目和错误，以及位、字节和冲突数等。

■　**VPN 统计和连接图**

通过支持 Cisco IPSec 流量监控 MIB，提供对 VPN 连接的全面显示，每个隧道的具体统计数据，包括隧道正常运行时间和所传输的字节/分组数。

17.1.2　Cisco ASDM 初始化

1.　开始前的准备

在开始运行“Startup Wizard”（启动向导）之前，先执行下述操作。

① 获得一个 DES 许可证或 3DES-AES 许可证。

> **提·示**
> 运行 ASDM,必须拥有自适应安全设备的 DES 许可证或 3DES-AES 许可证。

② 在 Web 浏览器上启用 Java and Javascript。

③ 搜集下列信息：

- 在网络中能够识别自适应安全设备的主机名。
- 外部接口、内部接口和其他接口的 IP 地址信息。
- 用于 NAT 或 PAT 配置的 IP 地址信息。
- DHCP 服务器的 IP 地址范围。

2. 使用“Startup Wizard”初始化

ASDM 使用“Startup Wizard”简单地初始化自适应安全设备。只需很少的几个步骤，启动向导就可以启用自适应安全设备，实现数据在内部接口和外部接口的安全传输。

① 使用跳线将安装并运行 Cisco ASDM 的管理计算机与 Cisco ASA 的管理接口 Mangement 0/0 连接在一起（如图 17-8 所示），或者将计算机与 Cisco ASA 连接至同一网段。ASA 5505 则使用非 Ehterbet 0/0 以外的其他以太网接口。

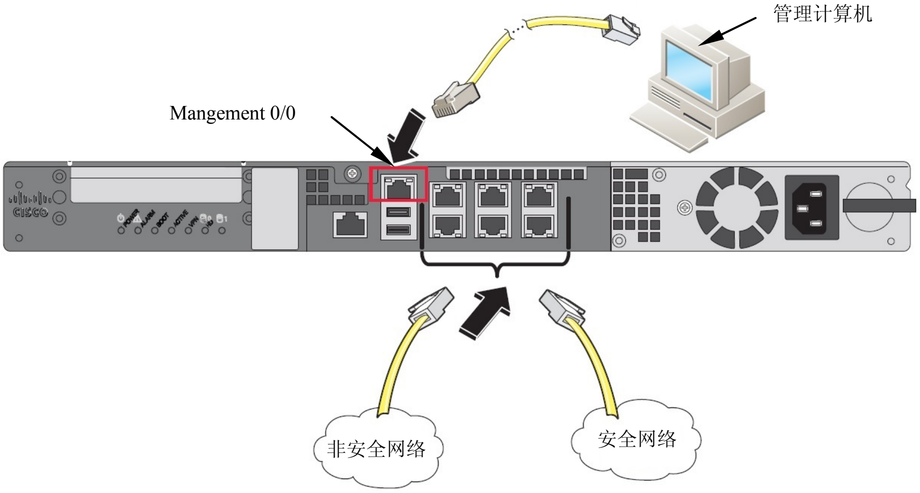


图 17-8 管理计算机与 Cisco ASA 的连接

> **提·示**
> 如果使用 CLI 初始化 Cisco ASA，则应当连接至 Console 端口。

② 配置计算机使用 DHCP 方式，将自动从自适应安全设备获得 IP 地址信息。

> **提·示**　自适应安全设备的内部接口默认被指定为 192.168.1.1。

③ 检查前面板的 Power LED 指示灯，如果呈稳定的绿色，则 Cisco 的电源已经开启。另外，再检查 Status LED 指示灯，当呈现为稳定的绿色时，表明系统加电诊断已经顺利完成。同时，当连接正常时，Mangement 接口的 LINK LED 指示灯也应当呈绿色。

④ 运行“Startup Wizard”启动向导。在计算机上运行 Web 浏览器，在“地址”栏中键入 https://192.168.1.1/admin 并按 Enter 键。

⑤ ADSM 启动（如图 17-9 所示）。单击“Run Startup Wizard”按钮，运行 Cisco ASDM 配置向导。

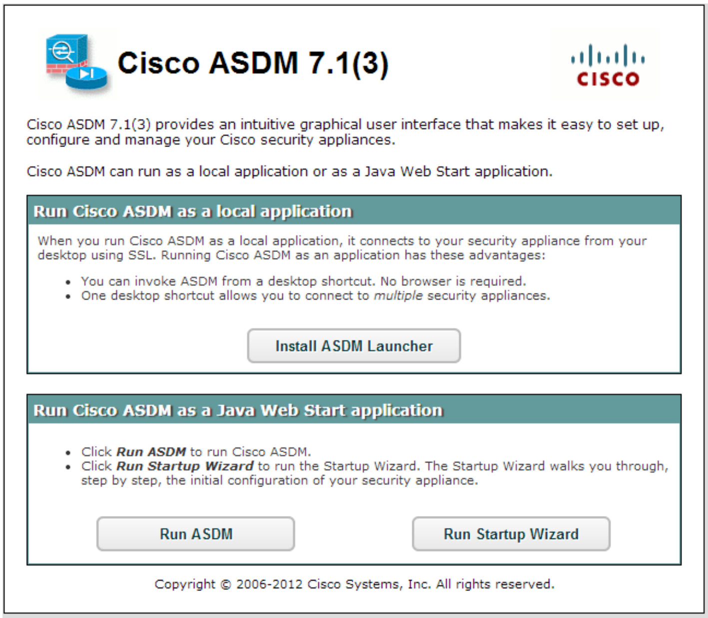


图 17-9　Cisco ASDM 启动

⑥ 单击“Yes”按钮，同意安装数字证书，并在随后的所有确认对话框中全部单击“Yes”按钮。

⑦ 对话框中需要键入用户名和密码，不过默认为空。因此，可以直接进入。

⑧ 根据启动向导中的提示，设置自适应安全设备。

> **提·示**　在 ASDM 主窗口的菜单“Wizards”中单击“Startup Wizard”命令，可以重新运行该配置向导。

17.1.3 配置 Cisco ASDM 访问

若欲访问 Cisco ASA 的 ASDM，需要先完成一些最小配置，然后，才能通过管理接口穿越网络与之进行通信。

1. 使用出厂默认配置访问 ASDM

在出厂默认配置情况下，ASDM 能够通过默认网络设置连接到 ASA。连接 ASDM 使用下列接口和网络配置：

- 模块上的管理接口。ASA 5505 的任何交换接口都可以连接到 ASDM，不过，推荐使用 Ehternet 0/0。ASA 5510 及更高的机型使用 Management 0/0 端口连接。
- 默认管理地址为 192.168.1.1。
- 客户端必须位于 192.168.1.0/24 网络，才被允许访问 ASDM。ASA 默认配置为启用 DHCP，因此，管理工作站能够被分配一个 IP 地址。

2. 使用非默认配置访问 ASDM

如果不是出厂默认配置，或者想修改至透明防火墙模式，应当执行下述操作。

①（可选）启用透明防火墙模式。该命令将清除配置。

```
hostname(config)# firewall transparent
```

② 在路由模式下，配置接口所属 VLAN、IP 地址和子网掩码、接口名称和安全级别。security-level 的取值范围为 1～100，100 为最安全。

```
hostname(config)# interface vlan number
hostname(config-if)# ip address ip_address [mask]
hostname(config-if)# nameif name
hostname(config-if)# security-level level
```

或者，在透明模式下，配置桥接虚拟接口，并为该桥组分配一个管理 VLAN。

```
hostname(config)# interface bvi number
hostname(config-if)# ip address ip_address [mask]

hostname(config-if)# interface vlan number
hostname(config)# bridge-group bvi_number
hostname(config-if)# nameif name
hostname(config-if)# security-level level
```

③ 启用管理交换端口，并将其分配至管理 VLAN。

```
hostname(config)# interface ethernet 0/n
hostname(config-if)# switchport access vlan number
hostname(config-if)# no shutdown
```

④ 在管理接口网络为管理主机启用 DHCP 服务。确认 DHCP 分配的 IP 地址范围中不包含 ASA 管理地址。

```
hostname(config)# dhcpd address ip_address-ip_address interface_name
hostname(config)# dhcpd enable interface_name
```

⑤ 为 ASDM 启用 HTTP 服务。

```
hostname(config)# http server enable
```

⑥ 允许管理主机访问 ASDM。

```
hostname(config)# http ip_address mask interface_name
```

⑦ 保存修改的配置。

```
hostname(config)# write memory
```

⑧ 在管理工作站运行 ASDM。

17.2 Cisco ASDM 配置防火墙

17.2.1 DMZ 配置

网络拓扑结构如图 17-10 所示。该结构具有如下特征。

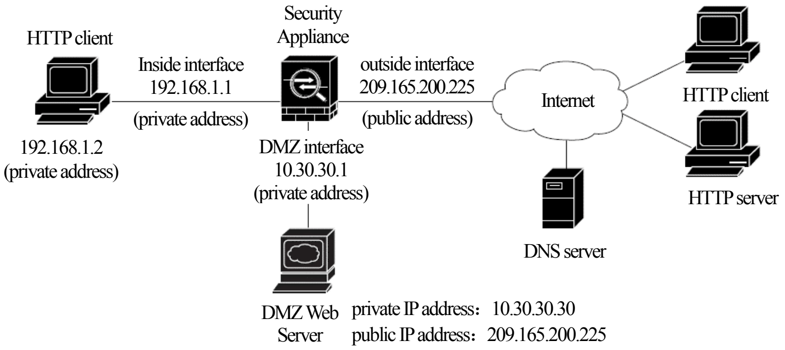


图 17-10 DMZ 拓扑结构

Web 服务器连接至安全设备的 DMZ 接口。

- HTTP 客户端位于私有网络，可以访问位于 DMZ 中的 Web 服务器，并且可以访问 Internet 中的设备。
- Internet 中的 HTTP 客户端允许访问 DMZ 区的 Web 服务器，除此之外的其他所有的通信都被禁止。
- 网络有两个可路由的 IP 地址可以被公开访问：安全设备外部端口的 IP 地址为 209.165.200.225，DMZ 中 Web 服务器的公开 IP 地址为 209.165.200.226。

1. 运行 ASDM

打开 Web 浏览器，在"地址"栏中键入安全设备出厂默认的 IP 地址"https://192.168.1.1/admin/"，运行 Cisco ASDM 程序，显示 Cisco ASDM 主窗口，如图 17-11 所示。

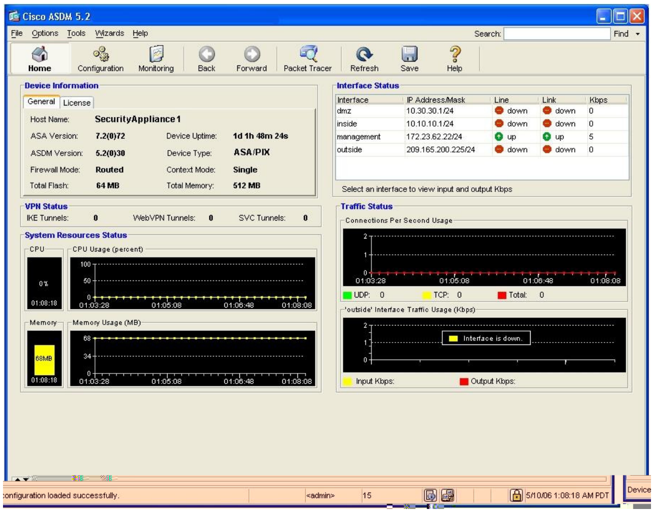


图 17-11　Cisco ASDM 主窗口

2.　为 NAT 创建 IP 地址池

安全设备使用 NAT（Network Address Translation，网络地址转换）和 PAT（Port Address Translation，端口地址转换）防止内部 IP 地址暴露在外部网络或 Internet。下面介绍如何为 DMZ 接口和外部接口创建一个可以被转换的 IP 地址池。

> **提示**：一个 IP 地址池可以同时包含 NAT 和 PAT 条目，也可以包含 1 个以上接口的条目。

■ 指定 DMZ 的 IP 地址范围

① 在 ASDM 窗口工具栏中，单击“Configuration”图标。然后在左侧栏中单击“NAT”图标，显示如图 17-12 所示的页面。

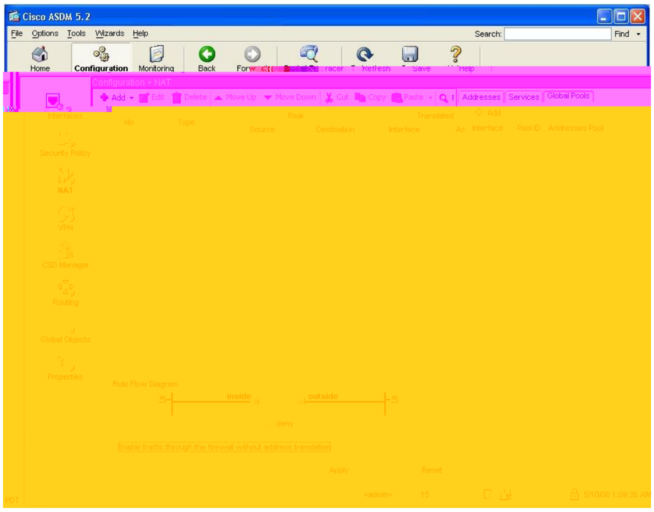


图 17-12　“NAT”图标

② 在右侧栏中打开“Global Pools”选项卡，单击“Add”按钮，显示“Add Global Address Pool”对话框，如图 17-13 所示，为 DMZ 接口创建一个新的全局地址池。

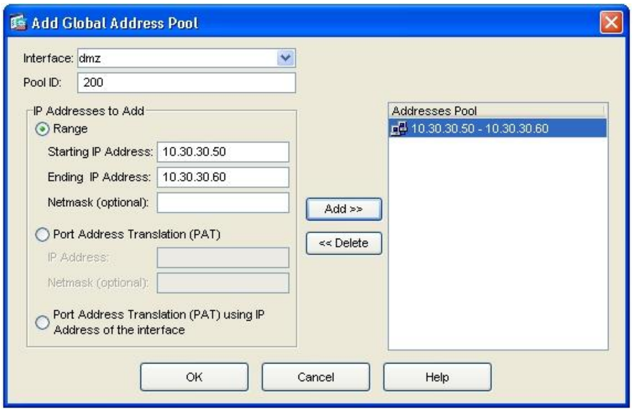


图 17-13 “Add Global Address Pool”对话框

③ 从“Interface”下拉列表中选择“dmz”选项，在“Pool ID”文本框中键入新创建地址池的 ID 号，如 200。

④ 在“IP Addresses to Add”选项组中指定 DMZ 接口使用的 IP 地址范围。选中“Range”单选按钮，在“Starting IP Address”和“Ending IP Address”文本框中分别键入起始和终止的 IP 地址“10.30.30.50”和“10.30.30.60”，选中“Port Address Translation（PAT）”单选按钮，并在“Netmask（optional）”文本框中键入子网掩码。

⑤ 单击“Add”按钮，将该 IP 地址范围添加至地址池。

⑥ 单击“OK”按钮，返回至“Configuration > NAT”窗口。

■ 为外部端口指定 IP 地址池

为外部端口指定 IP 地址，被用于转换私有 IP 地址，从而实现内部客户端对 Internet 的安全访问。借助 PAT 技术，可以使用同一合法 IP 地址将内部不同的服务器发布至 Internet。

① 在“NAT Configuration”窗口右侧，打开“Global Pools”选项卡，单击“Add”按钮，显示“Add Global Address Pool”对话框，如图 17-14 所示。

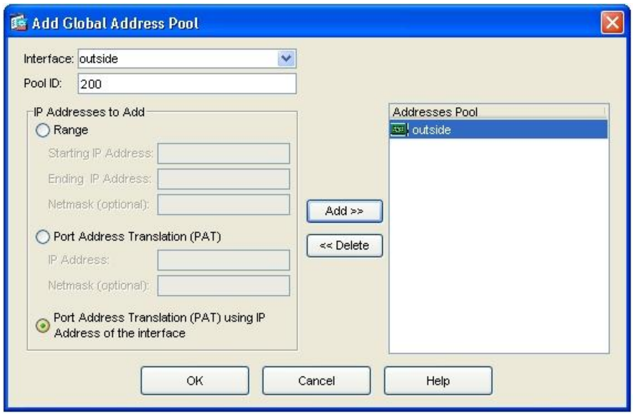


图 17-14 “Add Global Address Pool”对话框

② 在“Interface”下拉列表中选择“outside“选项，为外部接口指定地址池 ID 号，例如 200。可以将这些地址添加到与 DMZ 接口相同的 IP 地址池。

③ 选中“Port Address Translation（PAT）using IP Address of the interface”单选按钮，单击“Add”按钮将该地址添加至 IP 地址池。

④ 单击“OK”按钮，返回 Cisco ASDM 配置窗口，如图 17-15 所示。

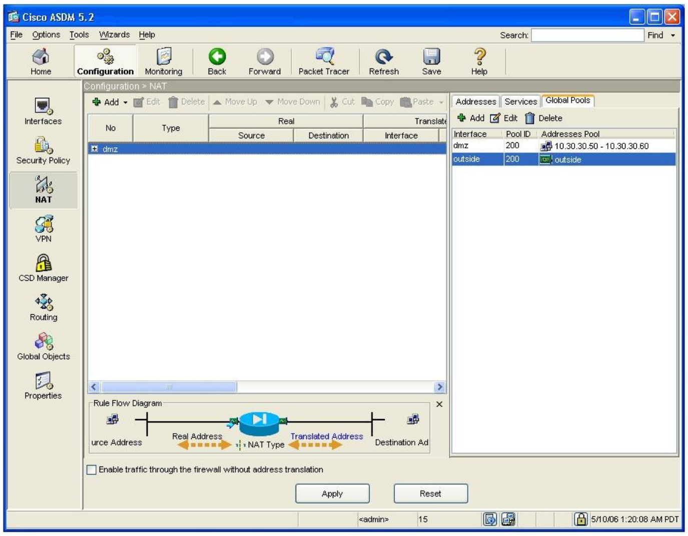


图 17-15　Cisco ASDM 配置窗口

确认配置无误后，在 ASDM 主窗口中单击“Apply”按钮。

3. 配置内部客户端访问 DMZ 区的 Web 服务器

在上述配置中，为内部客户端设置了安全的私有 IP 地址池。接下来将要配置一条 NAT 规则，用于实现内部客户端对 DMZ 区域中 Web 服务器的安全访问。

① 在 ASDM 主窗口工具栏中，单击“Configuration”图标。在左侧栏中单击“NAT”按钮，从“Add”下拉列表中选择“Add Dynamic NAT Rule”选项，显示“Add Dynamic NAT Rule”对话框，如图 17-16 所示。

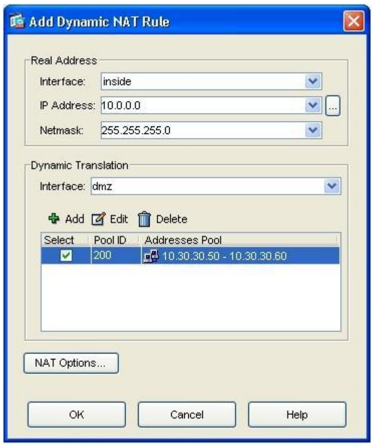


图 17-16　“Add Dynamic NAT Rule”对话框

② 在“Real Address”选项组中指定被转换的 IP 地址。从“Interface”下拉列表中选择“inside”选项，在“IP Address”文本框中键入内部客户端使用的 IP 网络号，如“10.10.10.0”，并在“Netmask”文本框中键入客户端网络的子网掩码，如“255.255.255.0”。

③ 在“Dynamic Translation”选项组中指定转换的目的 IP 地址。从“Interface”下拉列表中选择“dmz”接口，指定该地址池使用动态 NAT 规则。选中“Select”复选框，选择全局地址池 ID，例如“200”。

提·示　如果欲添加的地址池不存在，可以单击“Add”按钮创建新的 IP 地址池。

④ 单击“OK”按钮，添加动态 NAT 规则，并返回至“Configuration>NAT”窗口。ASDM 将添加 2 条规则，因为同一 IP 地址池同时被转换使用，如图 17-17 所示。

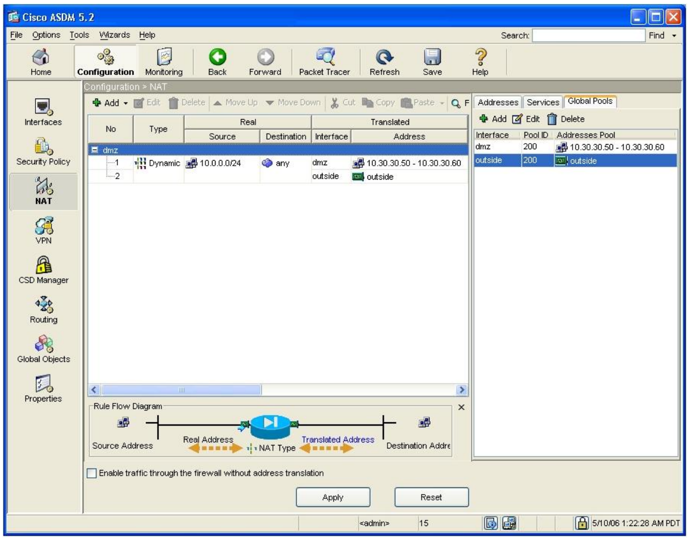


图 17-17　同时创建 2 条规则

4. 配置内部客户端访问 Internet

在上述配置中，借助 NAT 规则，可以实现内部客户端对 DMZ 区中 Web 服务器的访问。当然，借助 NAT 规则也应当能够实现内部客户端对 Internet 的访问。不过，管理员无需再创建任何规则了，因为 IP 地址池包括 2 种需要转换的地址，即 DMZ 接口使用的 IP 地址和外部接口使用的 IP 地址。可见，ASDM 已经自动为管理员创建了第 2 条转换规则。

5. 为 Web 服务器配置外部 ID

DMZ 中的 Web 服务器需要为 Internet 中所有的主机提供访问服务。该配置需要将 DMZ 中的 Web 服务器的私有 IP 地址转换为公有 IP 地址，允许外部 HTTP 客户端实现对 Web 服务的访问。借助以下操作，可以将真实的 Web 服务器的 IP 地址（10.30.30.30）静态映射为公有 IP 地址（209.165.200.226）。

① 在 ASDM 主窗口工具栏中，单击“Configuration”图标。在左侧栏中单击“NAT”按钮，从“Add”下拉列表中选择“Add Static NAT Rule”选项，显示“Add Static NAT Rule”对话框，如图 17-18 所示。

② 从“Interface”下拉列表中选择“dmz”接口，在“IP Address”文本框中键入 DMZ 区 Web 服务器的 IP 地址，如 10.30.30.30。在“Netmask”下拉列表中选择子网掩码“255.255.255.255”。

③ 在“Static Translation”区域指定 Web 服务器使用的公有 IP 地址。从“Interface”下拉

列表中选择“outside”选项，从“IP Address”下拉列表中选择 DMZ 区 Web 服务器使用的公有 IP 地址，如 209.165.200.226。

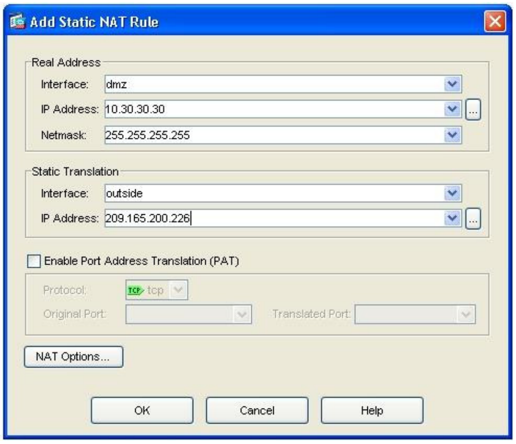


图 17-18 “Add Static NAT Rule”对话框

④ 单击“OK”按钮，添加规则，并返回至“Configuration＞NAT”窗口，如图 17-19 所示。该规则将真实的 Web 服务器的 IP 地址（10.30.30.30）静态映射为 Web 服务器的公有 IP 地址（209.165.200.226）。

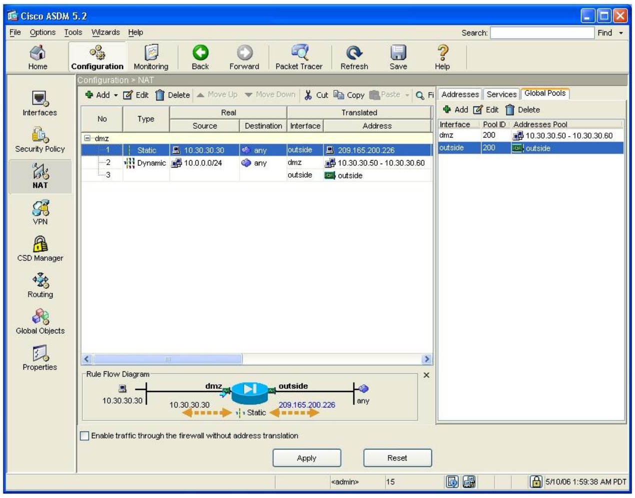


图 17-19 设置 Web 服务器公有 IP 地址映射

⑤ 单击“Apply”按钮，保存安全配置的修改。

6. 允许 Internet 用户访问 DMZ 的 Web 服务

默认情况下，安全设备禁止来自公共网络的所有通信。因此，必须创建一个安全规则，允许来自 Internet 用户对 DMZ 区中 Web 服务器的访问，即允许来源于 Internet 任意用户的针对 DMZ 中 Web 服务器的流入和流出的 HTTP 通信。

① 在 ASDM 主窗口工具栏中，单击“Configuration”图标。在左侧栏中单击“Security Policy”按钮，从“Add”下拉列表中选择“Add Access Rule”选项，显示“Add Access Rule”对话框，如图 17-20 所示。

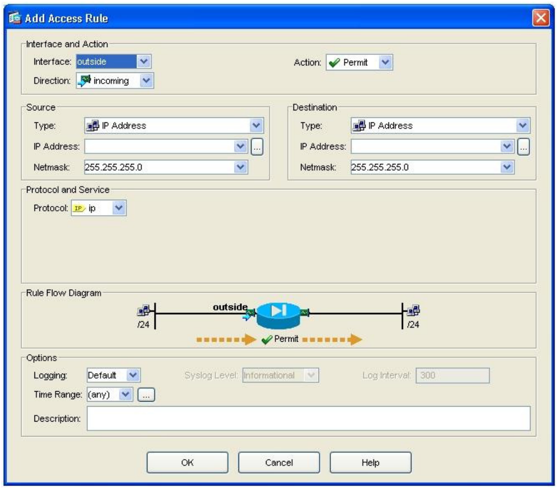


图 17-20　“Add Access Rule”对话框

② 在“Interface and Action”选项组中设置接口及允许的行为。在“Interface”下拉列表中选择“outside”选项，从“Direction”下拉列表中选择“incoming”选项，从“Action”下拉列表中选择“Permit”选项。

③ 在“Source”选项组中设置允许发起访问的源 IP 地址。在“Type”下拉列表中选择“IP Address”选项，在“IP Address”文本框中键入源主机或源网络的 IP 地址，使用“0.0.0.0”表示允许来自任何主机或网络的所有通信，在“Netmask”文本框中键入源 IP 地址的子网掩码。

④ 在“Destination”选项组中设置允许访问的目的 IP 地址。在“Type”下拉列表中选择“IP Address”选项，在“IP Address”文本框中键入目的主机或网络的公有 IP 地址，作为 DMZ 中 Web 服务器的 IP 地址，如 209.165.200.226，在“Netmask”文本框中键入子网掩码。

⑤ 在“Protocol and Service”选项组中指定允许传输的类型。在“Protocol”下拉列表中选择“tcp”选项。在“Source Port”区域，选中“Service”单选按钮，并在左侧的下拉列表中分别选择“=”和“any”选项。在“Destination Port”区域，选中“Service”单选按钮，并在左侧的下拉列表中分别选择“=”和“http/www”选项。完成后的配置页面如图 17-21 所示。

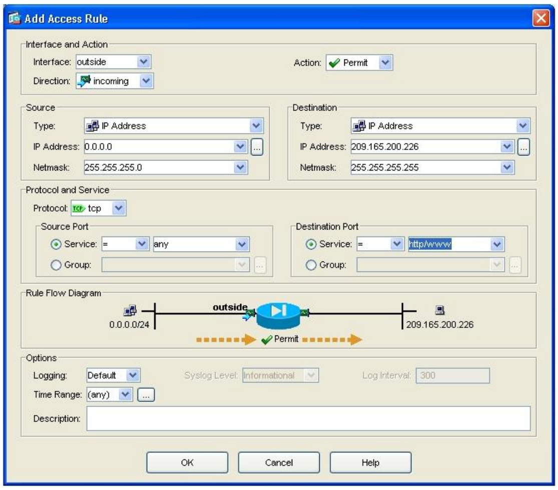


图 17-21　配置 Internet 客户访问

⑥ 确认无误后，单击“OK”按钮，返回 Cisco ASDM 主页面（如图 17-22 所示），再次校验配置信息是否正确。

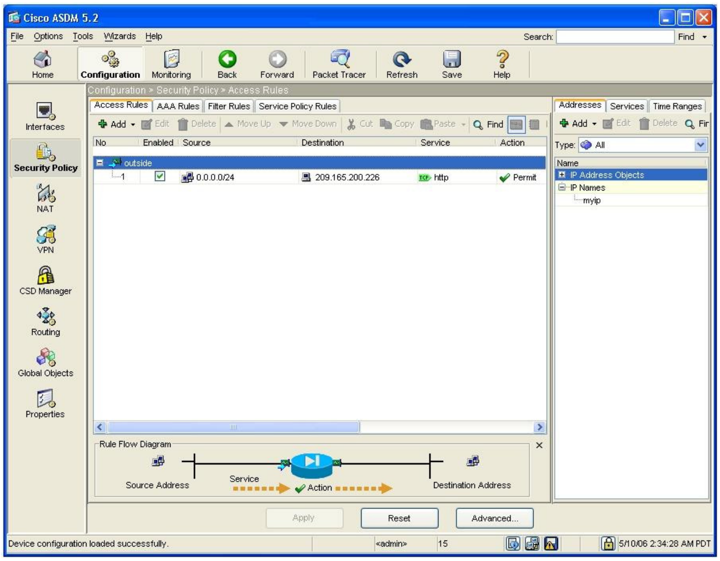


图 17-22　Cisco ASDM 主页面

⑦ 单击“Apply”按钮，保存对配置的修改。此时，私有网络和 Internet 中的所有客户端，将都可以访问 DMZ 区中的 Web 服务了。

17.2.2 IPsec VPN 远程访问配置

IPsec VPN 远程访问非常适用于远程移动用户，借助 Internet 或其他公用网络，实现与公司网络的安全、廉价的连接。图 17-23 所示为 IPsec VPN 远程访问的拓扑结构。

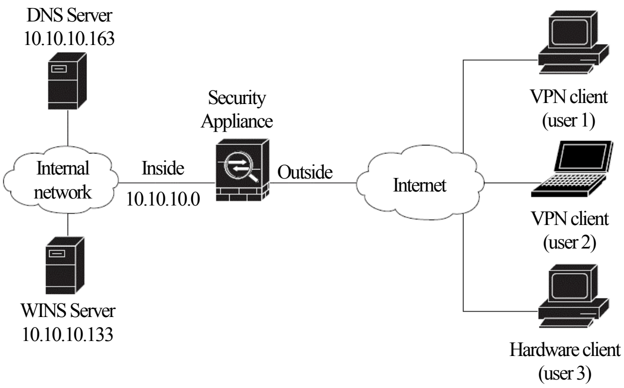


图 17-23　IPsec VPN 远程访问的拓扑结构

在配置 IPsec VPN 远程访问之前，确认已经准备好以下信息。

- IPsec VPN 远程客户端使用的 IP 地址池范围。
- 在本地认证数据库中创建用户列表，或者使用 AAA 服务器实现认证。
- 当 VPN 连接时，远程客户端使用的网络信息，包括：

- ➢ 主 DNS 服务器和辅助 DNS 服务器的 IP 地址。
- ➢ 主 WINS 服务器和辅助 WINS 服务器的 IP 地址。
- ➢ 默认域名。
- ➢ 认证远程客户端可访问的本地主机、组和网络的 IP 地址列表。

① 运行 ASDM。打开 Web 浏览器，在“地址”栏中键入安全设备出厂默认的 IP 地址“https://192.168.1.1/admin/”，运行 Cisco ASDM 程序，显示 Cisco ASDM 主窗口。

② 在 PIX 515E 上配置 IPsec 远程访问。在 ASDM 窗口，从“Wizard”菜单中选择“VPN Wizard”命令，运行 VPN 向导，显示“VPN Tunnel Type”对话框，如图 17-24 所示。选中“Remote Access”单选按钮，从“VPN Tunnel Interface”下拉列表中选择“outside”选项。

图 17-24 “VPN Tunnel Type”对话框

③ 单击“Next”按钮，显示如图 17-25 所示的“Remote Access Client”对话框，选择 VPN 客户端类型。在这里，选中“Cisco VPN Cleint, Release 3.x or higher, or other Easy VPN Remote product”单选按钮。当然，也可以根据需要选择其他 Cisco Easy VPN 远程产品。

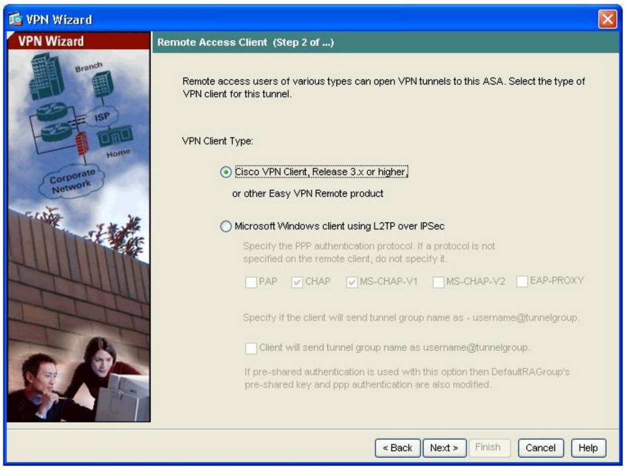


图 17-25 “Remote Access Client”对话框

④ 单击“Next”按钮，显示如图 17-26 所示的“VPN Client Authentication Method and Tunnel

Group Name”对话框，指定 VPN 隧道组名称和认证方式。

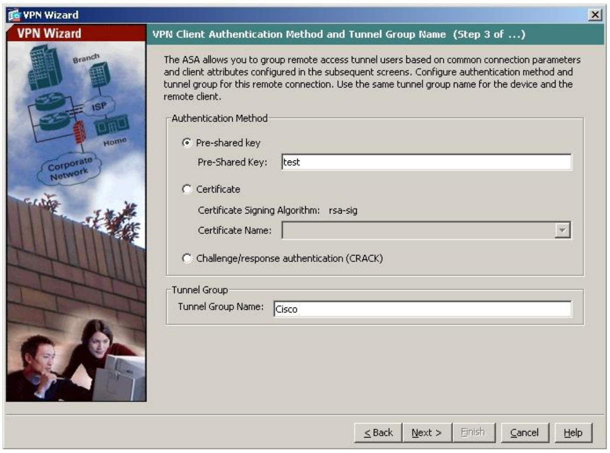


图 17-26 “VPN Client Authentication Method and Tunnel Group Name”对话框

可选的认证方式包括：

- 选中“Pre-shared key”单选按钮，使用预先分享的静态密钥认证，在“Pre-Shared Key”文本框中键入预先分享密钥。该密钥将在两个相邻的 IPsec 安全设备协商时被使用。
- 选中“Certificate”单选按钮，使用数字证书认证，从“Certificate Signing Algorithm”下拉列表中选择相应的算法。
- 选中“Challenge/response authentication（CRACK）”单选按钮，使用该方式进行验证。

在“Tunnel Group Name”文本框中键入隧道组名称，确定用户使用公共连接的参数和连接至该安全设备的客户端属性。

⑤ 单击“Next”按钮，显示如图 17-27 所示的“Client Authentication”对话框，指定用户认证方式。若欲通过在安全设备上创建用户数据库的方式实现用户验证，选中“Authenticate using the local user database”单选按钮。若欲使用外置的 AAA 服务器组实现用户验证，则选中“Authenticate using an AAA server group”单选按钮，并在“AAA Server Group Name”文本框中键入 AAA 服务器组的名称。

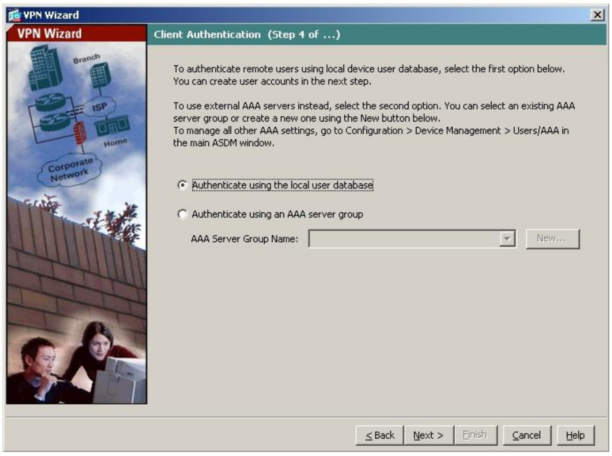


图 17-27 “Client Authentication”对话框

⑥（可选）单击“Next”按钮，显示如图 17-28 所示的“User Accounts”对话框，如果选择本地用户数据库验证用户，则可以在这里创建新用户账号，也可以稍后使用 ASDM 配置界面添加用户。在“Username”、“Password”和“Confirm Password”文本框中分别键入用户名、密码、校验密码，然后单击“Add”按钮，即可向本地用户数据库中添加新的用户。重复操作，可添加多名用户。

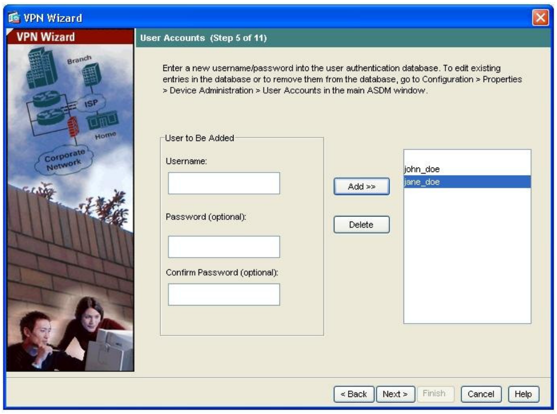


图 17-28 “User Accounts”对话框

⑦ 单击“Next”按钮，显示如图 17-29 所示的“Address Pool”对话框。

单击“New”按钮，显示如图 17-30 所示的“Address IP Pool”对话框，设置远程 VPN 用户访问网络时自动分配的 IP 地址范围，分别在“Name”、“Starting IP Address”、“Ending IP Address”和“Subnet Mask”文本框中键入 IP 地址池名称、起止 IP 地址和子网掩码，如“RemoteClientPool”、“209.165.201.1”、“209.166.201.20”和“255.255.255.0”。单击“OK”按钮返回。

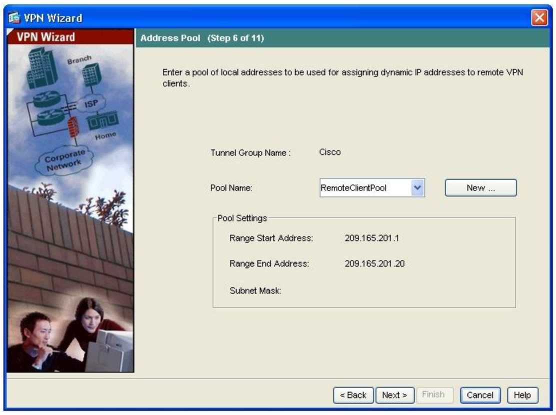


图 17-29 “Address Pool”对话框

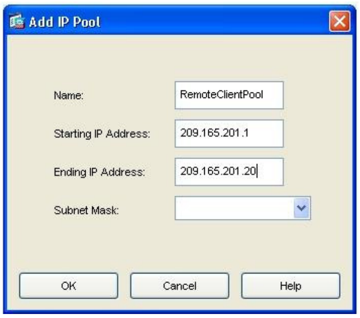


图 17-30 “Address IP Pool”对话框

⑧ 单击“Next”按钮，显示如图 17-31 所示的“Attributes Pushed to Client（Optional）”对话框，配置客户基本网络属性。当远程 VPN 用户访问网络时，都需要基本的网络配置信息，例如 DNS、WINS 服务器的 IP 地址和默认域名等。与其为每个用户单独配置，不如直接在 ASDM 中进行统一配置，这样当远程客户端或 Easy VPN 硬件客户端访问到网络时，将会自动获得这些基本网络信息。

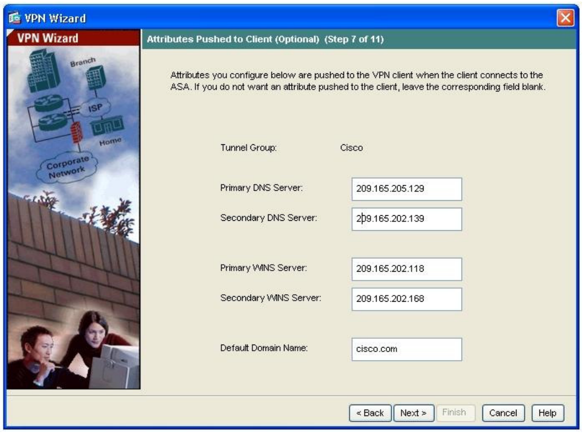


图 17-31 “Attributes Pushed to Client (Optional)”对话框

⑨ 单击“Next”按钮，显示如图 17-32 所示的“IKE Policy”对话框，配置 IKE 策略。IKE 是一个协商协议，既包括数据加密方式，也包括认证方式。分别在“Encryption”、“Authentication”和“DH Group”下拉列表中选择加密方式（DES/3DES/AES）、认证算法（MD5/SHA）和 Diffie-Hellman 组（1/2/5/7）。采用 ADSM 系统默认值，将足以在远程客户端与安全设备之间创建安全的 VPN 隧道。

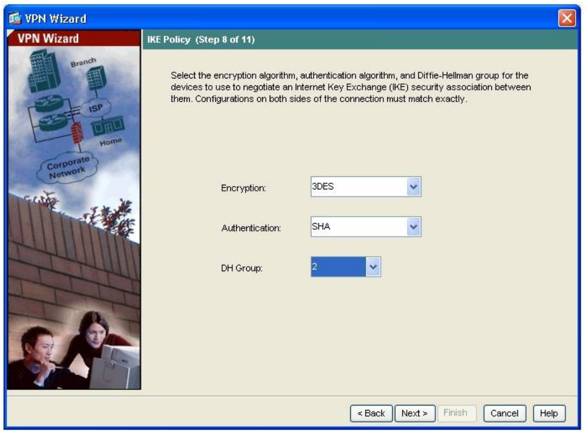


图 17-32 “IKE Policy”对话框

⑩ 单击“Next”按钮，显示如图 17-33 所示的“IPsec Encryption and Authentication”对话框，配置 IPsec 加密和认证参数。分别在“Encryption”和“Authentication”下拉列表中选择加密算法（DES/3DES/AES）和认证算法（MD5/SHA）。

⑪ 单击“Next”按钮，显示如图 17-34 所示的“Address Translation Exemption and Split Tunneling”对话框，指定转换例外地址和分割隧道（Split Tunneling）。分割隧道可以让远程访问 IPsec 客户端时有条件地将包直接在一个加密的 IPsec 隧道中传输。安全设备使用 NAT 预防内部 IP 地址暴露在外部网络中，不过，也可以设置被经过认证的远程用户访问的本地主机或网络的保护例外。本例中，设置 10.10.10.0 网络中所有的主机被暴露于所有远程客户端面前。在“Interface”下拉列表中选择“inside”选项，在“Address”文本框中键入欲暴露的 IP 地址或网络，单击“Add”按钮添加至列表。

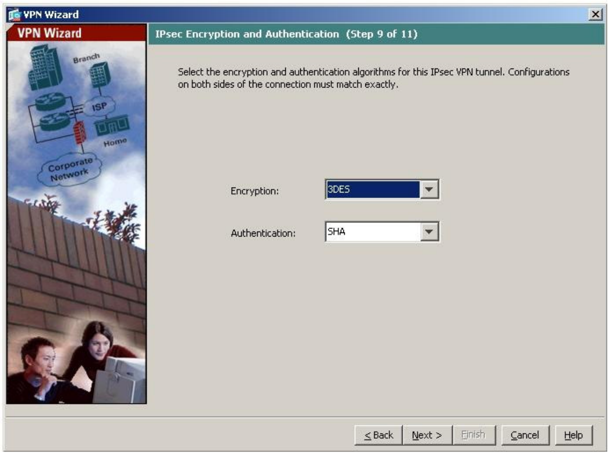


图 17-33　“IPsec Encryption and Authentication”对话框

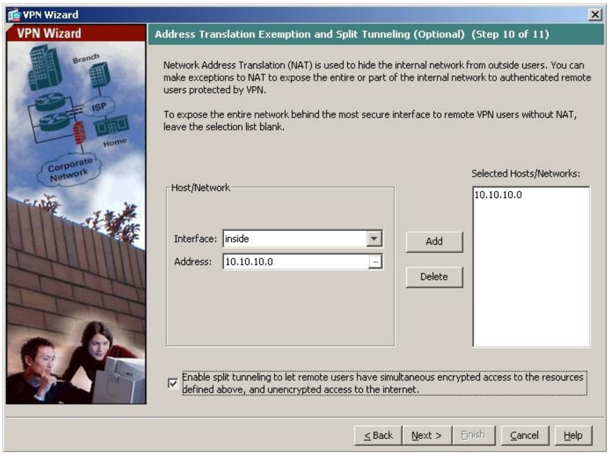


图 17-33　“Address Translation Exemption and Split Tunneling”对话框

⑫ 单击“Next”按钮，显示如图 17-35 所示的“Summary”对话框，显示 VPN 配置信息汇总。

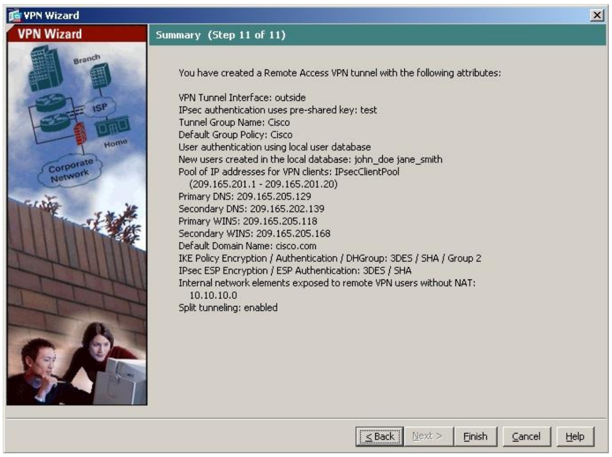


图 17-35　“Summary”对话框

确认无误后，单击“Finish”按钮，完成 VPN 配置并保存。

17.2.3 Site-to-Site VPN 配置

借助 Site-to-Site VPN 配置，可以实现远程网络廉价安全的互连，特别适用于总公司与分部之间的相互连接。图 17-36 所示为网络层的 Site-to-Site VPN 拓扑结构。

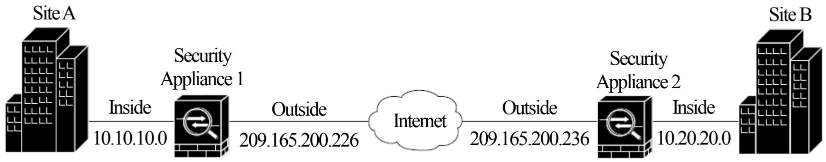


图 17-36　Site-to-Site VPN 拓扑结构

在开始配置之前，应当确认已经准备好以下数据。

- 对端远程安全设备的 IP 地址。
- 允许使用隧道连接与远程站点上的资源通信的本地主机和网络的 IP 地址。
- 允许使用隧道与本地资源通信的远程主机和网络的 IP 地址。

① 运行 ASDM。打开 Web 浏览器，在“地址”栏中键入安全设备出厂默认的 IP 地址“https://192.168.1.1/admin/”，运行 Cisco ASDM 程序，显示 Cisco ASDM 主窗口。

② 配置本地站点安全设备。在 ASDM 窗口，从“Wizard”菜单中选择“VPN Wizard”命令，运行 VPN 向导，显示“VPN Tunnel Type”对话框。选中“Site-to-Site”单选按钮（如图 17-37 所示），从“VPN Tunnel Interface”下拉列表中选择“outside”选项。

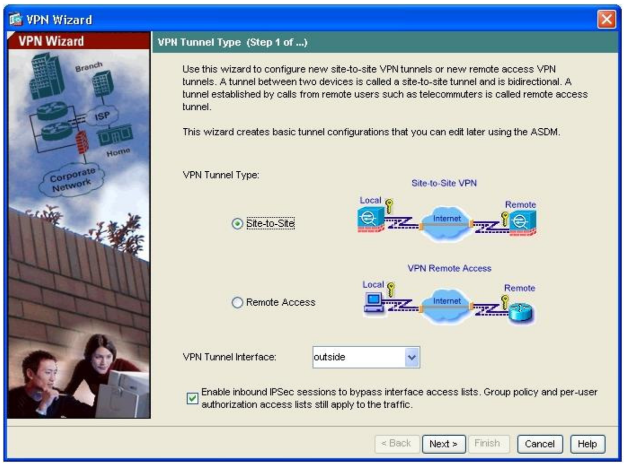


图 17-37　“VPN Tunnel Type”对话框

③ 单击“Next”按钮，显示如图 17-38 所示的“Remote Site Peer”对话框，在“Peer IP Address”文本框中键入对端安全设备的 IP 地址（如 209.165.200.236），并在“Authentication Method”选项组中选择认证方式。具体认证方式的选择，请参见上述相关内容，在“Tunnel Group Name”文本框键入隧道组名称。

④ 单击“Next”按钮，显示如图 17-39 所示的“IKE Policy”对话框，配置 IKE 策略。采用 ASDM 的系统默认值，将足以在两个安全设备之间创建安全的 VPN 隧道。

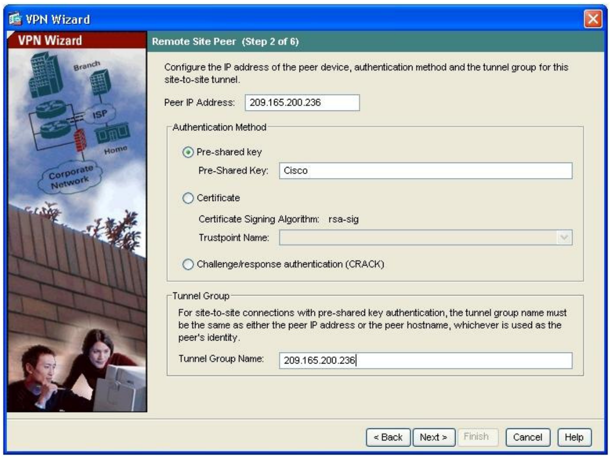


图 17-38 “Remote Site Peer”对话框

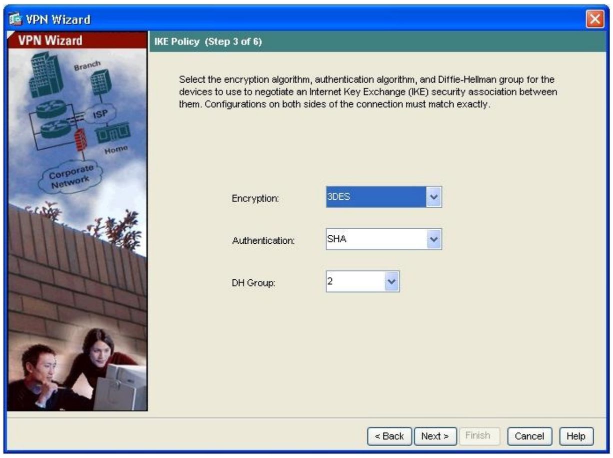


图 17-39 “IKE Policy”对话框

⑤ 单击“Next”按钮，显示如图 17-40 所示的“IPsec Encryption and Authentication”对话框，配置 IPsec 加密和认证参数。详细设置，请参见上述相关内容。

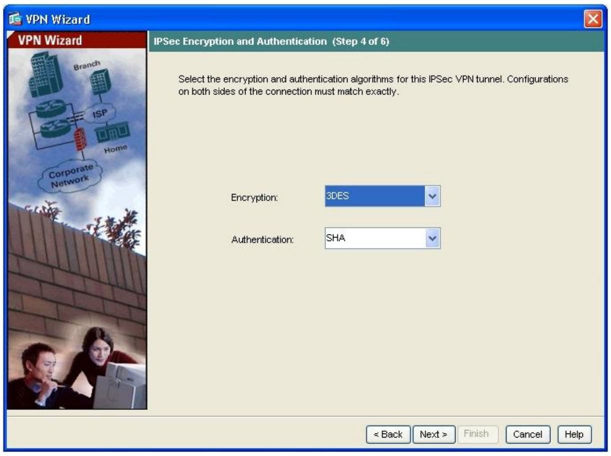


图 17-40 “IPsec Encryption and Authentication”对话框

⑥ 单击“Next”按钮，显示如图 17-41 所示的“Hosts and Networks”对话框，指定主机和网络。在“Source”选项组中，标识本地站点中允许使用 IPsec 隧道访问远程站点的主机和网络。在“Type”下拉列表中选择“IP Address”选项，在“IP Address”和“Netmask”下拉列表框中分别键入本地网络的 IP 地址和子网掩码。在“Destination”选项组中，标识远程站点中允许使用 IPsec 隧道访问本地站点的主机和网络。在“Type”下拉列表中选择“IP Address”选项，在“IP Address”和“Netmask”下拉列表框中分别键入远程网络的 IP 地址和子网掩码。

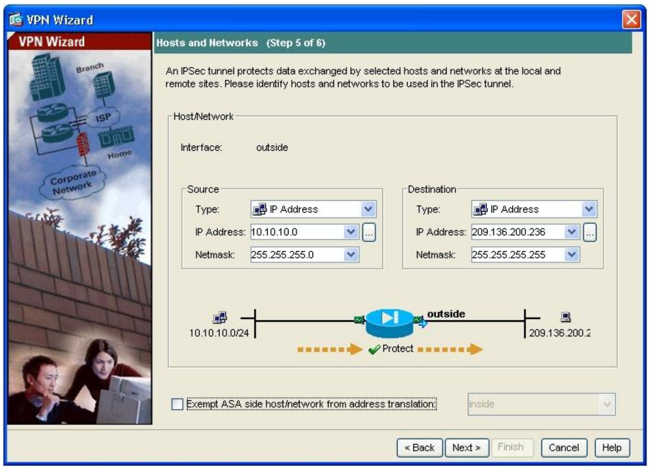


图 17-41 “Hosts and Networks”对话框

⑦ 单击“Next”按钮，显示如图 17-42 所示的“Summary”对话框，显示 VPN 配置的汇总信息。

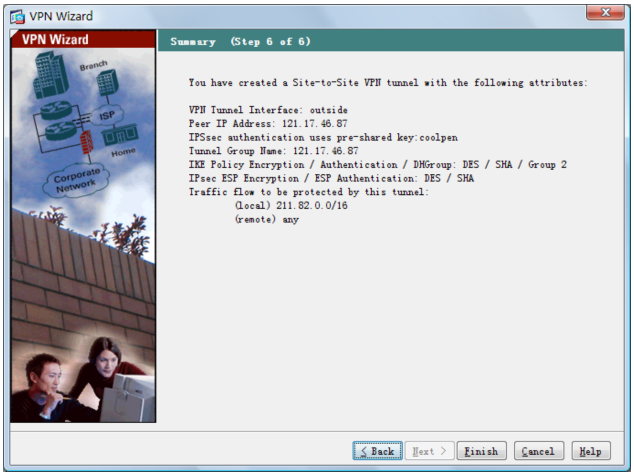


图 17-42 “Summary”对话框

⑧ 确认无误后，单击“Finish”按钮，返回 ADSM 主窗口。若欲将修改后的配置保存至启用配置（Startup Configuration），当设备下一次启动时应用，那么还应当在“File”菜单中选择“Save”命令。

⑨ 配置对端另一台 VPN 设备，应当确保两端的相关参数保持一致。

17.3 管理安全设备

使用 Cisco 自适应安全设备管理器管理安全设备，可以通过 Web 图形界面监视设备的运行状态、查看和分析网络流量、查看和分析系统日志及安全监控工具，使管理员能够更好地管理安全设备。

17.3.1 监视安全设备运行状态

利用 Cisco ASDM 登录到 Cisco ASA 主界面（见图 17-43），在 Device Dashboard 选项卡中显示了设备仪表板的信息，包括设备信息（名称、版本、型号等）、系统资源运行状态（CPU 和 Memory）、接口状态和信息传输状态。

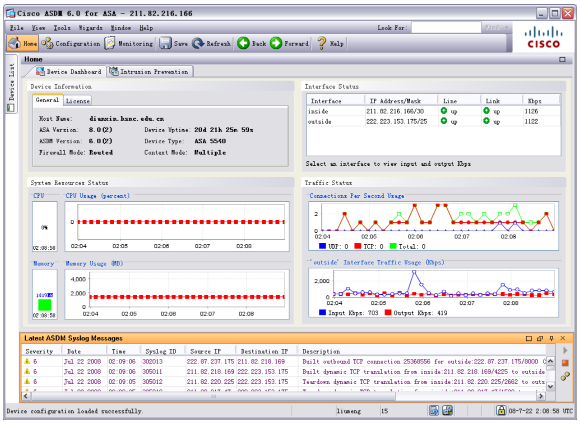


图 17-43　Cisco ASA 主界面

17.3.2 查看和分析网络流量

① 在 Cisco ASA 主界面中单击 Monitoring 按钮，监视设备的接口信息，如图 17-44 所示。

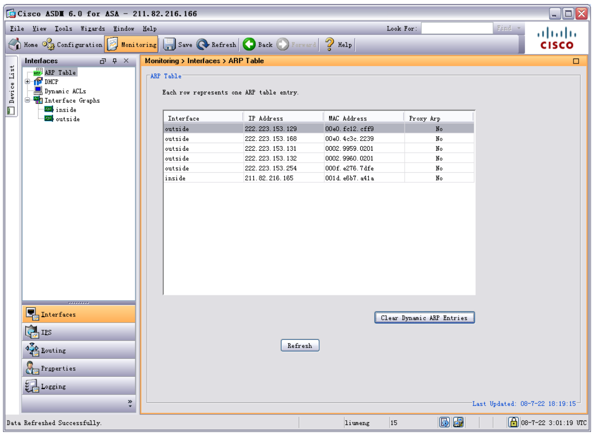


图 17-44　监视设备的接口信息

② 在左侧窗格中选择 Interfaces→Interface Graphs 选项，可以查看内部或外部的接口图表，如图 17-45 所示。

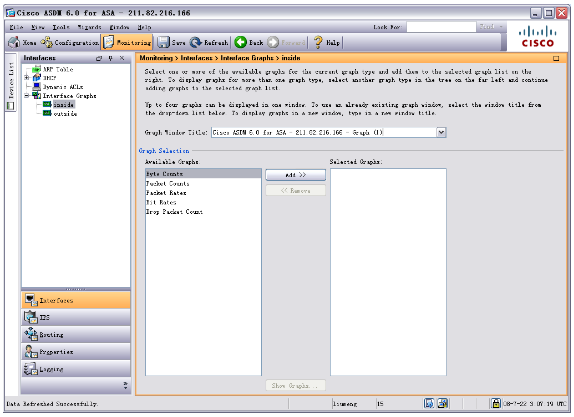


图 17-45 Interface Graphs 窗口

③ 以 inside 为例，在 Graph Selection 选项区域中显示图形所选内容，在 Available Graphs 列表框中选择可用图形并添加到 Selected Graphs 列表框中，如图 17-46 所示。

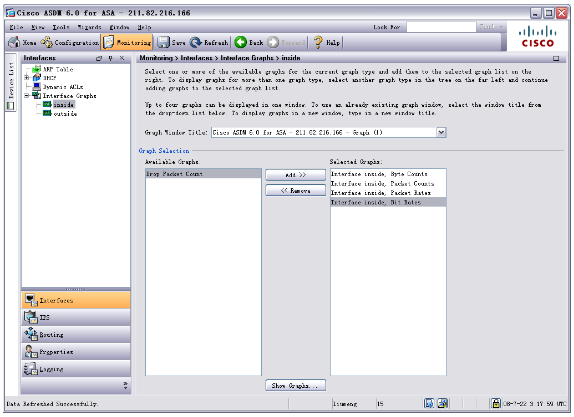


图 17-46 Graph Selection 选项区域

④ 单击 Show Graphs 按钮，以图例形式显示网络的流量，如图 17-47 所示。

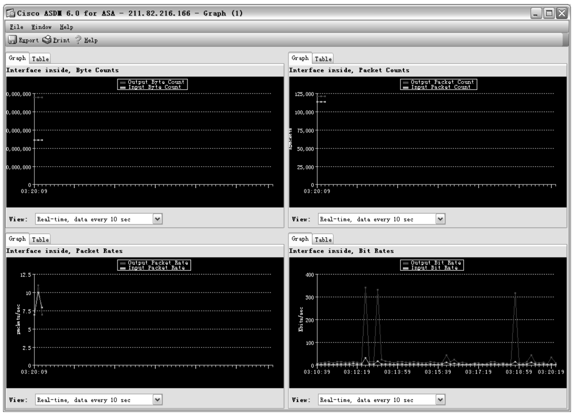


图 17-47 网络流量

17.3.3 查看和分析系统日志

① 在 Cisco ASA 主页左窗格中选择 Logging 选项，打开如图 17-48 所示的 Real-Time Log Viewer 窗口，在 Logging Level 下拉列表中选择日志记录级别。在 Buffer Limit 文本框中输入缓冲区限制，一般为默认值即可。

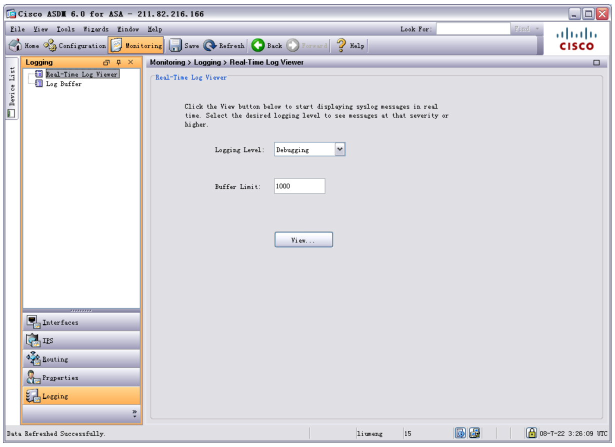


图 17-48 Real-Time Log Viewer 窗口

② 单击 View 按钮，系统日志以视图方式显示，如图 17-49 所示。

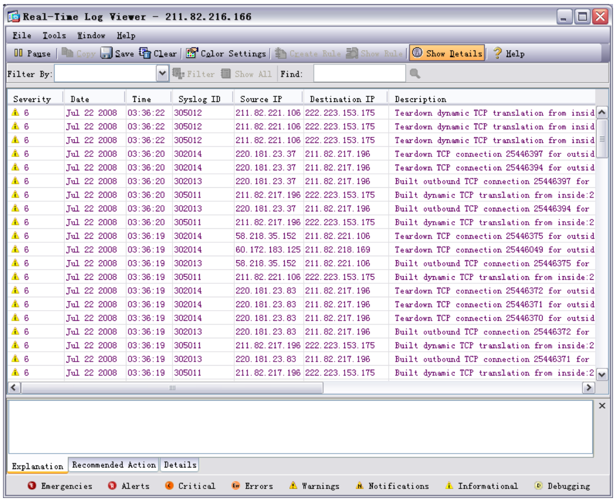


图 17-49 系统日志

第 18 章　使用 CLI 配置管理防火墙

与 Cisco 交换机和路由器一样，Cisco ASA 网络防火墙也可以使用 CLI 进行配置和管理，而且大多数命令（尤其是涉及到交换和路由配置方面的命令）与交换机和路由器完全相同，只有少量 Cisco ASA 网络防火墙独有的命令，因此，使用 CLI 配置更加快捷和高效。

18.1　配置的管理与恢复

在 ASA 配置出现问题，或者需要对 ASA 进行重新配置时，先将 ASA 恢复为出厂默认值，然后，再做进一步的处理无疑是最快捷和有效的方法。

18.1.1　Cisco ASA 默认配置

1. Cisco ASA 5505 路由模式默认配置

Cisco ASA 5505 默认出厂配置如下：

- 接口——内部（inside）VLAN 1 和外部（outside）VLAN 2。
- 交换端口启用和指定——Ethernet 0/1 至 Ethernet 0/7 交换端口被指定为内部(inside)，Ethernet 0/0 被指定为外部。
- IP 地址信息——外部 IP 地址信息来自 DHCP，内部地址被手工设置，IP 地址和子网掩码分别为 192.168.1.1 和 255.255.255.0。
- 网络地址转换（Network Address Translation，NAT）——当访问外部时，所有内部 IP 地址使用 PAT 转换为外部 IP 地址。
- 通信流量（Traffic Flow）——默认情况下，内部用户可以访问外部，外部用户被禁止访问内部。
- DHCP 服务——为内部主机启用，所以，当计算机连接至内部接口时，将自动获得范围在 192.168.1.5～192.168.254 中的 IP 地址。DNS、WINS 和域信息从外部接口的 DHCP 客户端获得，并传送给内部接口的 DHCP 客户端。
- 默认路由——从 DHCP 获取。
- ASDM 访问——允许内部主机访问。

图 18-1 所示为 ASA 5505 路由模式下的数据传输。

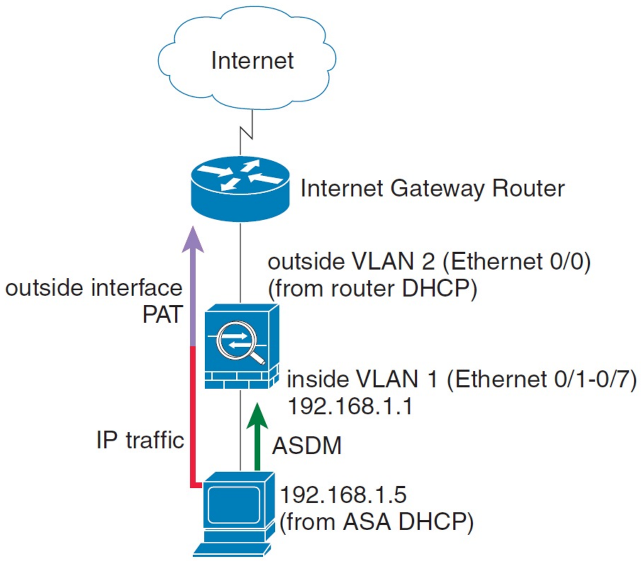


图 18-1 ASA 5505 路由模式下的数据传输

ASA 5505 路由模式的默认配置为：

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
```

```
  nameif inside
  ip address 192.168.1.1 255.255.255.0
  security-level 100
  no shutdown
object network obj_any
  subnet 0 0
  nat (inside,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

2. Cisco ASA 5505 透明模式范例配置

当将 ASA 5505 修改为透明模式时，配置将被删除。可以在 CLI 命令行下拷贝粘贴下列范例配置，作为默认配置的起点，并在此基础上根据需要做适当地修改。以下内容可能需要做必要的修改：

- IP 地址——该 IP 地址应当与所连接的网络相匹配。
- 静态路由——对于某些类型的通信，必须配置静态路由。

图 18-2 所示为 ASA 5505 透明模式下的数据传输。

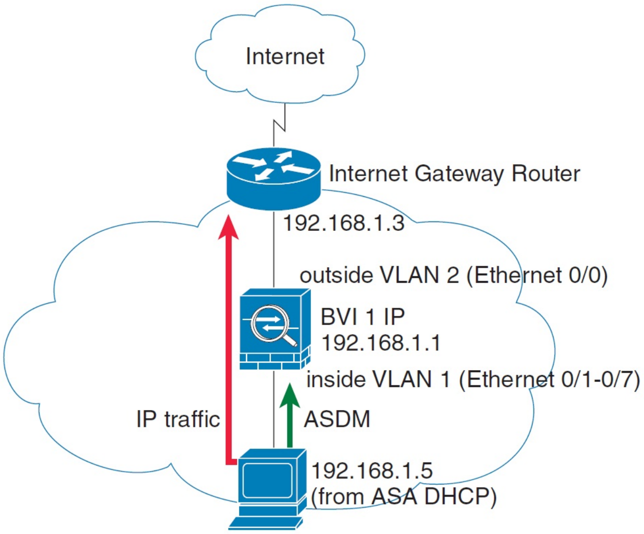


图 18-2　ASA 5505 透明模式下的数据传输

ASA 5505 透明模式的范例配置为：

```
firewall transparent
interface Ethernet 0/0
  switchport access vlan 2
  no shutdown
interface Ethernet 0/1
  switchport access vlan 1
```

```
  no shutdown
interface Ethernet 0/2
  switchport access vlan 1
  no shutdown
interface Ethernet 0/3
  switchport access vlan 1
  no shutdown
interface Ethernet 0/4
  switchport access vlan 1
  no shutdown
interface Ethernet 0/5
  switchport access vlan 1
  no shutdown
interface Ethernet 0/6
  switchport access vlan 1
  no shutdown
interface Ethernet 0/7
  switchport access vlan 1
  no shutdown
interface bvi 1
  ip address 192.168.1.1 255.255.255.0
interface vlan2
  nameif outside
  security-level 0
  bridge-group 1
  no shutdown
interface vlan1
  nameif inside
  security-level 100
  bridge-group 1
  no shutdown
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
```

3. Cisco ASA 5510 和更高产品默认配置

Cisco ASA 5510 和更高产品的默认出厂配置如下：

- 管理接口——Management 0/0。
- IP 地址——如果没使用 configrue factory-default 命令重新设置 IP 地址信息，其 IP 地址和子网掩码分别为 192.168.1.1 和 255.255.255.0。
- DHCP 服务器——默认被启用，因此，计算机连接至管理接口时，将自动获得范围在 192.168.1.2～192.168.254 中的 IP 地址。
- ASDM 访问——允许管理主机访问。

配置由下列命令组成：

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
```

```
    nameif management
    security-level 100
    no shutdown
 asdm logging informational 100
 asdm history enable
 http server enable
 http 192.168.1.0 255.255.255.0 management
 dhcpd address 192.168.1.2-192.168.1.254 management
 dhcpd lease 3600
 dhcpd ping_timeout 750
 dhcpd enable management
```

18.1.2 恢复出厂默认配置

恢复出厂默认设置只有在 ASA 处于路由防火墙模式时可用，透明模式不支持接口的 IP 地址。另外，该功能只在单一环境模式（Context）下有效。

在全局模式下，恢复至出厂默认设置。如果需要指定 IP 地址，可以设置 inside 或管理接口的 IP 地址，用于代替原来默认的 IP 地址 192.168.1.1。

```
ASA(config)# configure factory-default [ip_address [mask]]
```

18.1.3 ASA 配置的保存和管理

由于 ASA 可以划分为若干个虚拟防火墙，因此，在保存和管理配置时，便于交换机和路由器有所不同。

1. 保存修改的配置

■ **在单一环境模式下保存修改的配置**

将默认配置保存至闪存作为启动配置。write memory 与 copy running-config startup-config 命令等效。

```
ASA# write memory
```

■ **在多环境模式下保存修改的配置**

若欲保存系统或多个环境（Multiple Context，即多个虚拟防火墙）的配置，既可以进入系统或环境（即虚拟防火墙）执行 write memory 命令，也可以同时保存所有的环境和系统配置。命令格式为：

```
ASA# write memory all [/noconfirm]
```

如果没有输入/noconfirm 关键字，将显示如下提示：

```
Are you sure [Y / N]
```

输入 Y 后，ASA 保存系统配置和每个环境。环境启动配置可以保存于外部服务器。在 ASA

保存每个环境时，将显示类似下述信息：

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

2. 启动配置与运行配置

借助下述命令，可以复制新的启动配置至当前运行配置，使启动配置与运行配置相融合，其结果是从启动配置中添加所有新的命令至运行配置。如果配置相同，将不会有任何改变。如果命令有冲突，或者命令影响环境的运行，那么融合所造成的影响将由命令而定。当然，可能会导致错误，甚至是无法预料的结果。

```
ASA# copy startup-config running-config
```

重新装载 ASA，将装载启动配置，并丢弃运行配置。

```
ASA# reload
```

在无需重新引导 ASA 系统的情况下，装载启动配置并丢弃运行配置。

```
ASA# clear configure all
ASA# copy startup-config running-config
```

查看运行配置。

```
ASA# show running-config
```

查看运行配置中指定的命令。

```
ASA# show running-config command
```

查看启动配置。

```
ASA# show startup-config
```

3. 清除或移除配置

使用 clear configure *configurationcommand* 命令，清除指定命令的所有配置。如果只想清除配置中某个指定的更为具体的命令，则应当进一步指定值 *level2configurationcommand*。例如，若欲清除配置中所有的 aaa 命令，只需输入 clear configure aaa，而欲只清除配置中的 aaa authentication 命令，则应当输入 clear configure aaa authentication。

```
ASA(config)# clear configure configurationcommand [level2configurationcommand]
```

若欲禁用命令的某个参数或选项，可以使用 no 命令移除以 qualifier 标记的指定配置。

```
ASA(config)# no configurationcommand [level2configurationcommand] qualifier
```

删除启动配置。

```
ASA(config)# write erase
```

删除所有运行配置。在多环境模式下，如果在系统配置中使用该命令，将移除所有环境并停止其运行。环境配置文件不被删除，并被保留在其原始位置。

```
ASA(config)# clear configure all
```

18.2　配置防火墙和安全环境模式

18.2.1 配置透明或路由防火墙

1. 透明防火墙模式

图 18-3 所示为典型的透明防火墙网络，外部设备与内部设备位于同一子网。内部的路由器和主机就像直接连接到外部路由器上一样。

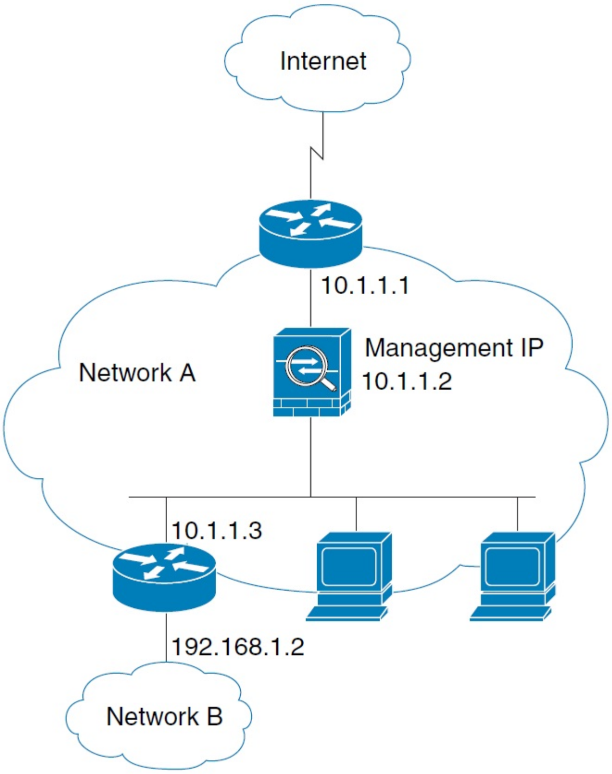


图 18-3　透明防火墙网络

2. 透明防火墙配置策略

■　**环境模式配置策略**

在配置 ASA 系统的环境模式时，应当遵循以下策略：

- ASA 默认模式为路由模式。
- 对于 ASA 5500 系列而言，防火墙模式的设置是针对整个系统和所有虚拟防火墙而言的，不能分别为每个虚拟防火墙分别设置模式。
- 在改变模式时，由于许多命令不能同时支持两种模式，因此，ASA 将清除运行配置，

同时，也将移除所有虚拟防火墙。如果此时重新添加已有配置的虚拟防火墙，那么，在创建时将处于错误模式，虚拟防火墙配置可能无法正确工作。因此，在重新添加虚拟防火墙时，应当确认是在正确的模式下重新创建，或者是在新的路径下以新的配置添加新的虚拟防火墙。

■ **透明防火墙配置策略**

在规划透明防火墙网络时，应当遵循以下策略：

- 在透明防火墙模式中，管理接口与数据接口一样，以同样的方式更新 MAC 地址表。因此，不要同时将管理接口和数据接口连接至同一台交换机，除非将其中一个配置为路由端口（默认情况下，Cisco Catalyst 交换机为所有的 VLAN 交换端口共享 MAC 地址）。否则，在通信从物理连接交换机到达管理接口时，ASA 将更新 MAC 地址表，并使用管理接口而不是数据接口访问交换机，从而将导致通信的暂时中断。由于安全方面的原因，在至少 30 s 的时间内，ASA 将不能再次从连接数据接口的交换机更新 MAC 地址表。
- 每个直连网络必须在同一子网。
- 不能指定桥组的管理 IP 地址作为默认网关以连接设备，而是应当指定 ASA 另一侧的路由器作为默认网关。
- 为透明防火墙指定默认路由，从而为管理通信提供返回路径。如果管理通信来自于多个桥组网络，必须指定静态路由以标识网络。

3. 配置步骤

使用 firewall transparent 命令，即可将 ASA 设置为透明模式。系统不会显示有关 ASA 模式改变的提示，修改将即刻生效。

```
ASA(config)# firewall transparent
```

若欲将 ASA 改变为路由模式，可以使用 no firewall transparent 命令。

```
ASA(config)# no firewall transparent
```

18.2.2 配置多环境模式

可以将一台 ASA 划分为若干虚拟设备，即所谓的安全环境（即虚拟防火墙）。每个虚拟防火墙都是一个自主设备，有自己的安全策略、接口和管理员。ASA 会为每个虚拟防火墙保存一个配置文件，以分别保存其策略和配置。这些配置文件既可以保存在本地，也可以保存在外部服务器上。多环境（Multiple Context）与多个独立设备非常相似。多环境模式能够支持的功能很多，包括路由表、防火墙、IPS 和管理。同样，也有一些功能不被支持，如 VPN 和动态路由协议。

> **提示** 当 ASA 被配置为安全环境（Security Context）时，IPsec 或 SSL VPN 不能被启用。因此，这些功能将是无效的。

1. 多环境模式配置限制

在配置多环境模式时，应当遵守以下限制性规定：

- 防火墙模式——在路由和透明防火墙模式下均可支持。
- 失效备援（Failover）——在多环境模式下，只支持 Active/Active 模式失效备援。
- 型号——不支持 ASA 5505。
- 不支持功能——在多环境模式下，不支持动态路由协议、VPN、多播路由、威胁侦测（Threat Detection）、电话代理服务器（Phone Proxy）、QoS 和统一通信。
- 其他——环境模式（单一或多个）不存储在配置文件中，即使其可以重新引导。如果需要将配置文件拷贝至另一个设备，应当在新设备上设置与其相匹配的模式。

2. 配置多环境模式操作流程

若欲配置多环境模式，应当执行下述操作：

① 启用多环境模式。

②（可选）配置资源管理等级。

③ 在系统中配置接口。

④ 配置安全环境。

⑤（可选）自动将 MAC 地址分配至环境接口。

⑥ 在环境中完成接口配置。

3. 启用或禁用多环境模式

默认情况下，ASA 处于单一环境模式。

当将单一模式转换为多模式时，ASA 会将运行配置转变为两个，一个是包含系统配置的新的启动配置，另一个是包含 admin 环境（在内置闪存的根目录中）的 admin.cfg 文件。原有的运行配置被保存为 old_running.cfg（在内置闪存的根目录中）。原有的启动配置不被保存。ASA 自动为 admin 环境添加至系统配置的入口，名称为“admin”。

借助 mode multiple 命令，可以将 ASA 由单一模式改变为多模式环境，并根据提示重新引导 ASA。

```
ASA(config)# mode multiple
```

若欲将 ASA 恢复至单一环境模式，应当先将旧的运行配置复制为启动配置，并将环境模式修改为单一模式。

① 将备份的原运行配置文件拷贝至当前启动配置。

```
ASA(config)# copy flash:old_running.cfg startup-config
```

② 将 ASA 设置为单一模式。

```
ASA(config)# mode single
```

4. 配置资源管理级别

资源管理级别的配置操作应当在系统执行空间中完成。使用 show resource types 命令，可

以查看资源类型及限制。表 18-1 所示为资源名称和限制。

表 18-1 资源名称和限制

资源名称	速率或并发	每环境最小和最大值	系统限制	描 述
mac-addresses	并发	N/A	65 535	透明防火墙模式下，MAC 地址表允许的 MAC 地址数
cons	并发或速率	N/A	并发连接：依平台不同 速率：N/A	任意两个主机之间的 TCP 或 UDP 连接，包括一个主机与多个其他主机的连接
inspets	速率	N/A	N/A	应用检视
hosts	并发	N/A	N/A	能够连接并通过 ASA 的主机
asdm	并发	最小 1min 最大 5min	N/A	ASDM 管理进程。ASDM 使用两个 HTTPS 连接，一个总是出现，另外一个只有在修改配置时才会出现。例如，系统限制 32 个 ASDM 进程，意味着限制了 64 个 HTTPS 连接。
ssh	并发	最小 1min 最大 5min	200	SSH 进程
syslogs	速率	N/A	N/A	系统日志消息
telnet	并发	最小 1min 最大 5min	100	Telnet 进程
xlates	并发	N/A	N/A	地址转换

资源管理级别的配置过程如下：

① 指定级别名称，进入级别配置模式。name 最多可以包括 20 个字符。若欲将限制设置为默认级别，可以使用 default 关键字。

```
hostname(config)# class name
```

② 设置所有资源为无限制。默认情况下，所有资源的默认级别为无限制。

```
hostname(config)# limit-resource all 0
```

或者，设置特别的资源限制。对于指定的资源来说，该限制设置将覆盖由 all 设置的限制配置。rate 字段用于设置某个资源的每秒速率。

```
hostname(config)# limit-resource [rate] resource_name number[%]
```

5. 配置安全环境

安全环境在系统配置中由环境名称、配置文件 URL 和虚拟防火墙使用的接口进行定义。在进行配置时，注意以下几点。

- 该操作必须在系统配置界面下进行。
- 对于 ASA 5500 而言，配置物理接口参数、VLAN 子接口和冗余接口建议参考下述“接口配置”部分内容。
- 如果没有 admin 环境（例如，已清除配置），那么，必须首先使用 admin-context *name* 命令指定 admin 环境名称。尽管该环境名称在现有配置中并不存在，但是，可以稍后使用 context *name* 命令匹配指定的名称，以完成 admin 环境配置。

具体操作如下：

① 添加或修改环境。Name 最多 32 个字符，且对大小写敏感。可以使用字母、数字、连字符，但是，不能以连字符开始或结束。“System”或“Null”是保留名称，不能使用。

```
ASA(config)# context administrator
```

② （可选）添加对该环境的描述。

```
ASA(config)# description text
```

③ 指定该环境使用的接口。在接口类型和端口号之间不要有空格。

输入该命令多次，可以指定不同的范围。使用 no 结构命令移除分配的接口时，包括接口在内的环境命令都将被从运行配置中移除。

透明防火墙模式允许少量接口直通通信，可以使用专用的管理接口，Managentet *slot/port*（物理接口、子接口、冗余接口或 EtherChannel）作为附加接口管理通信。即使包在 MAC 地址表中没有匹配项，管理接口也不会将包泛洪（Flood）出该接口。

在路由模式中，如果需要，可以将同一个接口指定至多个环境。

mapped_name 是为接口指定别名（包括文字和数字），用于在环境中替代接口 ID。换言之，如果不为接口指定映射名称，就需要在环境中直接使用接口 ID。而为安全起见，可能并不想某些环境管理员知晓该环境中使用的具体接口，因此，指定别名就成为必要。映射名称必须以字母开头，以字母或数字结尾，中间可以是字母、数字或下画线，如 int0, inta, int_0 均是正确的别名。

如果指定的是一个子接口范围，那么，也可以为其指定一个映射名称以进行匹配。映射名称中所指定接口范围的字母部分两端必须匹配，如接口范围为 int0-int10，如果输入 gig0/1.1-gig0/1.5 happy1-sad5，就是无效的命令；数字部分则必须包含与子接口相同的数量，如 gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100 所指定的范围都包含 100 个接口，是正确的表达，而 gig0/0.100-gig0/0.199 int1-int15 则所指定的范围不同，就是错误的。

设置映射名称后，在 show interface 命令中使用 visible 关键字可以查看真实的接口 ID。默认情况下，invisible 关键字只有在映射名称中可见。

分配一个物理接口。

```
ASA(config-ctx)# allocate-interface physical_interface [mapped_name] [visible
| invisible]
```

分配一个或多个子接口。

```
ASA(config-ctx)# allocate-interface physical_interface.subinterface [-physical
_interface.subinterface] [mapped_name[-mapped_name]] [visible | invisible]
```

④ 确定从哪个系统下载环境配置。在添加环境 URL 时，如果配置有效，系统将立即装载环境配置作为其运行配置。

> **提示**　应当在 config-url 之前输入 allocate-interface 命令。如果先输入 config-url 命令，ASA 将立即装载环境配置。如果环境配置中包含任何有关接口命令（尚未配置），这些命令都将失败。

文件名无需文件扩展名，尽管推荐使用扩展名“.cfg”。必须能够从 admin 环境到达保存配置文件的服务器。如果配置文件无效，将看到如下提示消息：

```
WARNING: Could not fetch the URL disk:/url
INFO: Creating context with default config
```

对于非 HTTP（S）位置，在指定 URL 后，可以切换至该虚拟防火墙，并在 CLI 下进行配置，输入 write memory 命令将文件写至 URL 位置。HTTP（S）为只读。有效的 URL 类型包括 disk *number* (闪存),ftp, http, https 或 tftp，如 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg。若欲变更 URL，需要再次输入 config-url 命令。

```
ASA(config-ctx)# config-url url
```

> **提·示** Admin 虚拟防火墙文件必须存储在内置闪存中。

⑤ （可选）为该虚拟防火墙指定资源级别（Resource Class）。如果没有指定级别，虚拟防火墙将属于默认级别。只能为虚拟防火墙指定一个资源级别。

```
ASA(config-ctx)# member class_name
```

⑥ （可选）在 Active/Active 失效备援中为该虚拟防火墙分配一个失效备援组。默认情况下，虚拟防火墙处于 group 1。Admin 环境必须处于 group 1。

```
ASA(config-ctx)# join-failover-group {1 | 2}
```

⑦ （可选）如果安装有 AIP SSM，为该虚拟防火墙分配一个 IPS 虚拟传感器。

```
ASA(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

6. 在环境和系统间切换

使用 Telnet 或 SSH 登录至系统执行空间（System Execution Space）或 admin 环境后，可以在环境（Context）之间进行切换，以进行配置和执行监控操作。运行配置就是在配置模式中正在编辑的配置，或者使用 copy 或 write 命令复制和写入的配置。当处于系统执行空间时，运行配置只由系统配置构成。例如，不能以 show running-config 命令查看所有运行配置（系统及所有环境），只能显示当前配置。

若欲在系统执行空间和环境（即虚拟防火墙）之间，以及不同环境之间进行切换，应当执行下述操作：

切换至环境，系统提示符将改变为 hostname/*name*#。

```
changeto context name
```

切换至系统，系统提示符将改变为 hostname #。

```
changeto system
```

7. 多模式配置示例

该配置示例的相关设置如下：

- 在虚拟防火墙中自动设置 MAC 地址。
- 设置默认级别限制为 10%，而不是没有限制。
- 创建 gold 资源级别。
- 设置 Admin Context 为“administrator”。
- 在内置闪存上创建名为“administrator”的虚拟环境，作为默认资源级别的一部分。
- 从 FTP 服务器添加两个环境作为 gold 资源级别的一部分。

具体配置过程如下：

```
hostname(config)# mac-address auto prefix 19
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/
0.115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/
test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/1.230-gigabitethernet0/1.235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/
sample.cfg
hostname(config-ctx)# member gold
```

18.2.3 管理安全环境

1. 移除安全环境

可以通过编辑系统配置移除一个虚拟防火墙。不能移除当前 admin 环境，除非使用 clear context 命令移除所有环境。

移除单个环境时，该环境下的所有环境命令都将被移除。

```
no context name
```

移除所有环境（包括 Admin Context）。

```
clear context
```

2. 修改为 Admin Context

系统配置中不包括任何网络接口或网络设置。当系统需要访问网络资源（如从服务器下载环境）时，会使用指派为 Admin Context 的环境。

Admin Context 像其他虚拟防火墙一样，除了用户登录至 Admin Context 之外，即拥有系统管理权限和访问系统及其他环境的权限。任何情况下，Admin Context 都不受限制，并且能够跟其他虚拟防火墙一样使用。不过，因为登录到 Admin Context 后将被授予高于其他虚拟防火墙的管理特权，因此，应当严格控制访问 Admin Context 的用户。

可以将任何环境设置为 Admin Context，只要其配置文件存储于内部闪存即可。任何能够连接到 Admin Context 的远程管理进程都可以设置，如 Telnet、SSH 或 HTTPS。只是在配置了新的 Admin Context 后，需要重新连接。

```
ASA(config)# admin-context context_name
```

提·示 少数命令，包括 ntp server，标识接口名称等只属于 Admin Context。如果将某个环境改变为 Admin Context，接口名称在新的 Admin Context 中将不存在，应当确认更新涉及该接口的所有系统命令。

3. 修改安全环境 URL

除非从新的 URL 重新装载配置，否则，不能修改安全环境 URL。ASA 将混合新的配置和当前运行配置。再次输入相同的 URL 时，也将混合已经保存的配置和当前运行配置。

混合时，将从新配置中添加所有新命令至运行配置。如果配置相同，则不会做任何修改。如果命令冲突，或者命令会影响当前环境的运行，那么，混合的结果将依命令而定。或许会得到错误提示，或许会产生无法预料的结果。如果运行配置为空（如服务器无效，导致配置从未下载），将使用新的配置。

如果不想混合配置，可以清除运行配置。当然，在从新的 URL 重新装载配置之前，任何通过该虚拟防火墙的通信都将被中断。

① （可选，如果不想混合配置）切换至指定虚拟防火墙，并清除其配置。

```
hostname(config)# changeto context name
hostname/ctx1(config)# clear configure all
```

② 切换至系统执行空间。

```
hostname/ctx1(config)# changeto system
hostname(config)#
```

③ 切换至欲修改 URL 的虚拟防火墙。

```
hostname(config)# context name
```

④ 输入新的 URL，系统将立即装载环境并开始运行。

```
hostname(config)# config-url new_url
```

4. 重新装载安全环境

可以通过两种方式重新装载：

- 清除运行配置，并导入启动配置。该操作将最大限度地清除与环境有关的属性，如连接和 NAT 表。
- 从系统配置中移除环境。该操作将清除附加属性，如内存分配，在发生故障时可能会有作用。不过，再将该环境添加回系统时，需要指定 URL 和接口。

借助下述操作，可以清除环境配置并重新装载虚拟防火墙，将从 URL 重新装载配置。

① 切换至欲重新装载的虚拟防火墙。

```
hostname(comfig)# changeto context name
hostname/ctx1(comfig)#
```

② 清除运行配置，并清除所有连接。

```
hostname/ctx1(config)# clear configure all
```

③ 重新装载配置。ASA 从系统配置中指定的 URL 复制配置。不能在虚拟防火墙中修改 URL。

```
hostname/ctx1(config)# copy startup-config running-config
```

若欲移除并重新添加环境后再重新装载虚拟防火墙，则需要执行以下操作：

① 移除安全环境。

② 配置安全环境。

具体操作，请参见上述相关内容，此处不复赘述。

18.2.4 监控安全环境

1. 查看环境信息

在系统执行空间，可以查看包括名称、分配接口和配置文件 URL 在内的环境列表。

查看所有环境。detail 选项用于查看添加信息。若欲查看某个虚拟防火墙的信息，应当指定其名称。count 选项用于查看虚拟防火墙的总数。

```
hostname# show context
Context Name     Interfaces                URL
*admin           GigabitEthernet0/1.100    disk0:/admin.cfg
                 GigabitEthernet0/1.101
Context          GigabitEthernet0/1.200    disk0:/contexta.cfg
                 GigabitEthernet0/1.201
Context          GigabitEthernet0/1.300    disk0:/contextb.cfg
                 GigabitEthernet0/1.301
Total active Security Contexts: 3
```

其中，Context Name 列为所有虚拟防火墙名称，名称前带有*号的环境为 Admin Context。Interface 列为指定至虚拟防火墙的接口。URL 列为 ASA 从哪个 URL 装载环境配置。

2. 查看资源分配

在系统执行空间，可以查看分配的每个资源的所有级别及其成员。detail 选项用于查看添加信息。

```
hostname# show resource allocation [detail]
Resource            Total         % of Avail
Conns [rate]        35000           N/A
Inspects [rate]     35000           N/A
Syslogs [rate]      10500           N/A
Conns              305000          30.50%
Hosts               78842           N/A
SSH                    35          35.00%
Telnet                 35          35.00%
Xlates              91749           N/A
All unlimited
```

其中，Resource 列为可以限制的资源名称。Total 列为分配至所有环境的资源总量，该量为同时发生的实例或每秒发生的实例的总数。如果在级别定义中指定的是百分比，ASA 将在显示时将转换其为绝对数值。% of Avail 列为分配至所有环境的总系统资源的百分比。如果资源已经被硬件系统限制，则显示为百分数；如果资源未被系统限制，将显示为 N/A。

3. 监视 SYN 攻击

ASA 使用 TCP 拦截阻止 SYN 攻击。TCP 拦截使用 SYN Cookies 算法阻止 TCP SYN 泛洪攻击。SYN 泛洪攻击通常由持续的来自被哄骗 IP 地址的 SYN 包所构成。SYN 包持续泛洪导

致服务器 SYN 队列注满，从而阻止来自服务连接的请求。当连接到达阈值初期，ASA 将作为服务器的代理服务器，为客户端的 SYN 请求产生一个 SYN-ACK 应答。当 ASA 接收到来自客户端的 ACK back 时，能够鉴定客户端并允许其连接至服务器。

借助以下命令，可以监视 SYN 攻击。

监视某个虚拟防火墙攻击速率。

```
show perfmon
```

监视某个虚拟防火墙使用 TCP 拦截的来源数量。

```
show resource usage detail
```

监视整个系统使用 TCP 拦截的来源数量。

```
show resource usage summary detail
```

18.3 配置接口

18.3.1 接口默认配置

1. 默认接口状态

接口默认状态与产品型号和环境模式有关。

在多环境模式中，所有指派的接口默认都处于启用状态。当然，既然通信要通过该接口，系统执行空间中的接口状态也应当处于启用状态。如果宕掉系统执行空间中的接口，那么，该接口在共享它的所有环境中都将被宕掉。

在单一模式或系统执行空间中，接口处于下述默认状态：

- 物理接口——Disable（未启用）。
- 冗余接口——Enable（启用）。若欲通信能够通过冗余接口，成员物理接口必须处于启用状态。
- 子接口——Enable（启用）。若欲通信通过子接口，物理接口必须处于启用状态。
- EtherChannel 接口——Enable（启用）。若欲通信通过 EtherChannel，端口汇聚组中的成员物理接口必须处于启用状态。

2. 默认速率和双工模式

默认情况下，铜缆接口（RJ-45）速度和双工模式被设置为自适应。

ASA 5550（插槽 1）的光纤接口和 4GE SSM 为固定速率，且不支持双工，不过，可以设置接口协商链路参数（默认）或不协商。

ASA 5580 和 5585-X 的光纤接口，速率被设置为自动链路协商。

3. 默认连接器类型

ASA 5550（插槽 1）、ASA 5510 及更高产品的 4GE SSM 提供两种类型的连接器，铜缆 RJ-45 和光纤 SFP。RJ-45 为默认连接类型，当然，也可以配置 ASA 使用光纤 SFP 连接器。

4. 默认 MAC 地址

默认情况下，物理接口使用烧录的 MAC 地址，所有物理接口的子接口使用相同的烧录 MAC 地址。

18.3.2 配置策略和限制

1. 防火墙模式策略

- 在透明模式下，每个虚拟防火墙或单模式设备最多可以配置 8 个桥组。
- 每个桥组可以容纳最多 4 个接口。
- 多环境模式下，处于透明模式的每个虚拟防火墙必须使用不同的接口，不能跨环境共享接口。

2. 失效备援策略

- 当使用冗余或 EtherChannel 接口作为失效备援链路时，必须在失效备援时对每个单元中事先进行配置。
- 如果使用冗余或 EtherChannel 接口作为正式链路，无需进行特殊配置，配置能够正常从主单元复制。
- 可以使用 monitor-interface 命令监视冗余或 EtherChannel 接口的失效备援，但是，应当确认引用了正确的逻辑冗余接口名称。
- 如果使用 EtherChannel 接口作为失效备援或正式链路，将阻止 out-of-order 包，EtherChannel 中将只有一个接口被使用。如果该接口失败，EtherChannel 中的下一个接口将被使用。在 EtherChannel 用于失效备援链路时，不能修改其配置。若欲修改，需要宕掉 EtherChannel，或暂时禁用失效备援。
- 尽管可以在一个端口汇聚链路上配置失效备援和正式链路，但是，该端口组不能与其他防火墙通信共享。

3. 冗余接口策略

- 可以配置最多 8 个冗余接口对。
- 在进行所有 ASA 配置时，都是引用逻辑冗余接口而不是成员物理接口。
- 既不能将冗余接口作为 EtherChannel 的一部分，也不能将 EtherChannel 作为冗余接口的一部分。不能使用冗余接口和 EtherChannel 接口中的同一物理接口，但是，如果它们不使用同一物理接口，可以在 ASA 上同时配置这两种类型。
- 如果宕掉活跃（Active）接口，备用（Standby）接口将改变为活跃状态。
- Management *slot/port* 接口不能作为冗余接口成员，也不能设置由非管理接口组成的冗余接口作为只管理接口（Management-only）。

4. EtherChannel 策略

- 可以最多配置 48 个 EtherChannel。

- 每个 EtherChannel 可以最多有 8 个活跃接口。可以将最多 16 个接口指定至一个端口汇聚组，其中只有 8 个接口处于活跃状态，其他接口可以作为现有接口失败时的备用链接。
- 端口汇聚中的所有接口必须拥有相同的类型和速率。第一个加入端口组的接口确定了相应的类型和速率标准。
- 连接至 ASA 5500 EtherChannel 的设备必须支持 802.3ad EtherChannel。例如，不能连接至 Catalyst 6500 系列交换机。
- 在所有 ASA 配置中，都将引用逻辑 EtherChannel 接口以代替成员物理接口。
- 不能使用冗余连接作为 EtherChannel 的一部分，同样，也不能使用 EtherChannel 作为冗余接口的一部分。不能使用冗余接口和 EtherChannel 接口中的同一物理接口，但是，可以在 ASA 上同时配置这两种类型，如果它们不使用同一物理接口。
- 在 4GE SSM 上不能使用接口作为 EtherChannel 的一部分。

> **提·示**
>
> 如果已经进行过配置，再想转换使用中的冗余接口或 EtherChannel 接口，建议离线进行配置，以将由此而导致的通信中断减小到最低程度。

18.3.3 接口配置操作流程

在配置接口时，建议执行以下操作流程：

① （多环境模式）在系统执行空间中完成所有任务。输入 changeto system 命令，可以从环境切换至系统执行空间。

② 启用物理接口，并根据需要修改其以太网参数。物理接口默认为 disable。

③ （可选）配置冗余接口对。一个逻辑冗余接口对由一个活跃物理接口和一个备用物理接口组成。当活动接口失败时，备用接口将改变为活跃状态，并开始传输数据。

④ （可选）配置 EhterChannel。EhterChannel 将多个以太网接口绑定至一个逻辑接口。

⑤ （可选）配置 VLAN 子接口。

⑥ （可选）在 ASA 5580 和 5585-X 上启用巨型帧支持。

⑦ （只适用多环境模式）在系统执行空间完成接口配置，将接口分配至虚拟防火墙，将 MAC 地址自动分配至虚拟防火墙接口。MAC 地址用于虚拟防火墙内部的包分类。如果共享接口，但是没有为每个虚拟防火墙指定唯一的 MAC 地址，将使用目的 IP 地址进行包分类。做为选择，可以手工为虚拟防火墙指定 MAC 地址。

⑧ 完成接口配置。

18.3.4 将正在使用的接口转换为冗余或 EtherChannel 接口

如果已经进行了配置，但是，想将正在使用的接口转换为冗余接口或 EtherChannel 接口，那么，在转换至逻辑接口前，将会有一段时间的通信中断。

1. 单模式配置步骤

推荐离线修改配置文件，然后，再重新导入。原因如下：

- 因为不能添加一个已命名的接口作为冗余或EtherChannel接口，必须先从接口移除其名称。当从接口移除名称时，任何涉及到该名称的命令都将被删除。由于涉及名称的命令会广泛地存在于配置之中并影响多种功能，无论在CLI中，还是在ADSM中，从正在使用的接口上移除名称，都将对配置造成严重影响。换句话说，在为新接口名称重新配置所有功能之前，将导致严重的通信中断。
- 离线修改配置可以在新的逻辑接口使用同一接口名称，从而无需触及有关新接口名称的功能配置，只需修改接口配置即可。
- 清除运行配置并立即应用新配置将最大限度地减少接口的中断时间，并无需等待配置接口的时间。

具体配置过程如下：

① 连接至ASA。如果使用失效备援，则连接至活跃的ASA。

② 如果使用了失效备援，使用no failover命令禁用它。

③ 使用more system:running-confg命令复制运行配置，并拷贝显示输出至文本编辑器（如记事本）。确认为原有配置保存了额外的拷贝，以便在编辑出错时进行恢复。

④ 在每个欲添加至冗余接口或EtherChannel接口的接口上，在interface命令下，剪切正在使用的接口配置部分命令，并粘贴至新创建的新逻辑接口。只有media-type、speed、duplex和flowcontrol命令除外，因为它们属于物理接口配置。

> **提示** 可以只将物理接口添加至EtherChannel或冗余接口，但是，不能为物理接口配置VLAN。确认添加至EtherChannel或冗余接口的所有接口的属性都相匹配。EtherChannel上所有接口的双工配置必须为全双工或自动。

⑤ 输入下述命令后，每粘贴一个接口配置命令部分，创建一个新的逻辑接口。

```
interface redundant number [1-8]
interface port-channel channel_id [1-48]
```

⑥ 将物理接口分配至新的逻辑接口。

冗余接口——两个物理接口必须是相同类型（无论原来是否在使用），同时，不能将Management接口分配至冗余接口。在新interface redundant命令下，输入下述命令：

```
member-interface physical_interface1
member-interface physical_interface2
```

EtherChannel接口——每个EtherChannel最多可以容纳16个物理接口，其中只有8个处于活跃状态，另外8个处于备用状态。在每个欲添加至EtherChannel的接口（无论原来是否在使用）上输入下述命令：

```
channel-group channel_id mode active
```

⑦ 使用 no shutdown 命令启用逻辑接口中原来未被使用的接口。

⑧ 在 ASA CLI 提示符下，依连接方式（Console 或 Remote）不同，分别执行下述操作。

Console 连接：

a） 复制全部新配置至剪贴板，包括修改接口部分。

b） 使用 clear configе all 命令，清除运行配置，ASA 通信中断。

c） 在提示符下粘贴新的配置，ASA 通信重新恢复。

远程连接：

a） 将新配置保存至 TFTP 或 FTP 服务器，并在 ASA 上将其复制至启动配置。当然，为了便于管理操作，可以在远程管理计算机上安装 TFPT 或 FTP 服务器。

b） 使用 write erase 命令，清除启动配置。

c） 输入 copy *url* starup-config 命令，将新配置复制至启动配置。

d） 使用 reload 命令，重新装载 ASA。不保存运行配置。

⑨ 使用 failover 命令，重新启用失效备援。

2. 多模式配置步骤

推荐离线修改系统和环境配置文件，然后，再重新导入。

① 连接至 ASA，并切换至系统空间。如果使用失效备援，则连接至活跃的 ASA。

② 如果使用了失效备援，使用 no failover 命令禁用。

③ 在系统中，使用 more system:running-confg 命令复制运行配置，并复制显示输出至文本编辑器（如记事本）。确认为原有配置保存了额外的拷贝，以便在编辑错误时进行恢复。

④ 获取所有欲使用新冗余或 EtherChannel 接口的环境配置拷贝。

⑤ 在系统配置中，创建新的冗余或 EtherChannel 逻辑接口，并确认在所有添加至逻辑接口的物理接口上输入了 no shutdown 命令。

⑥ 修改分配给每个新虚拟防火墙的新建冗余或 EtherChannel 逻辑接口。

⑦ 由于虚拟防火墙不使用映射名称，需要使用新建冗余或 EtherChannel 逻辑接口 ID 修改环境配置（虚拟防火墙使用映射接口名称无需任何改变）。

⑧ 复制新的环境配置文件覆盖原来的旧文件。该修改只影响启动配置，运行配置仍然使用原来的旧环境配置文件。

⑨ 在 ASA CLI 提示符下，依连接方式（Console 或 Remote）不同，分别执行相应的操作。具体操作，参见“单模式配置步骤”中的相关内容。

⑩ 使用 failover 命令，重新启用失效备援。

18.3.5 配置和管理冗余接口

冗余接口由一个物理接口对（一个活跃接口和一个备用接口）组成。当活动接口失败时，备用接口改变为活跃状态并开始进行数据传输。借助配置冗余接口，可以增强 ASA 的可用性。虽然该功能与设备级的失效备援有区别，但是，仍然不失为一种非常好的选择。

1. 配置冗余接口

配置冗余接口时，限制性条件如下：

- 所有成员接口必须具有相同的物理属性。
- 虽然可以配置冗余接口的延迟值，但是，默认情况下，ASA 将继承其所属成员的物理接口的延迟值，而该延迟值与接口的物理类型有关。
- 如果为物理接口配置了名称，那么，不能将其添加至冗余接口。必须使用 no nameif 命令移除其名称。
- 在多环境模式中，需要在系统执行空间中完成该操作。使用 changeto system 命令，可以切换至系统执行空间。

> **提·示**　如果在配置中使用了某个物理接口，那么，移除名称时将清除与该接口有关的所有配置。

具体配置步骤如下：

① 添加逻辑冗余接口，*number* 取值范围为 1～8。

```
hostname(config)# interface redundant number
```

> **提·示**　在配置逻辑接口的参数（如名称）之前，需要向冗余接口中至少添加一个成员接口。

② 向冗余接口中添加第一个成员接口。冗余接口不支持 Management *slot/port* 接口作为成员。在将物理接口添加至冗余接口之后，所有配置（如 IP 地址）都将被移除。

```
hostname(config-if)# member-interface physical_interface
```

③ 向冗余接口中添加第二个成员接口。应当确认第二个接口与第一个接口具有相同的物理属性。

```
hostname(config-if)# member-interface physical_interface
```

若欲移除一个成员接口，只需输入 **no member-interface** *physical_interface* 命令。不能从冗余接口中移除所有的接口，至少应当保留一个成员接口。

接下来要做的任务，包括：

- （可选）配置 VLAN 子接口。
- 在多环境模式，将接口分配至虚拟防火墙，并给环境接口自动分配唯一的 MAC 地址。
- 在单环境模式，完成接口配置。

2. 查看和改变活跃接口

默认情况下，活跃接口是配置中位列第一的有效接口。若欲查看哪个接口处于活跃状态，可以使用下述命令：

```
hostname# show interface redundantnumber detail | grep Member
```

若欲改变活跃接口，可以使用下述命令：

```
hostname# redundant-interface redundantnumber active-member physical_interface
```

18.3.6 配置和管理 EtherChannel

配置冗余接口时，限制性条件如下：

- 所有 EtherChannel 成员接口必须具有相同的类型、速率和双工模式。不支持半双工。
- 如果为物理接口配置了名称，那么，不能将其添加至 EtherChannel。必须使用 no nameif 命令移除其名称。
- 在多环境模式中，需要在系统执行空间中完成该操作。使用 changeto system 命令，可以切换至系统执行空间。

ASA 的 EtherChannel 具体配置过程与交换机相似，请参阅相关内容，此处不复赘述。

18.3.7 配置相同安全级别通信

默认情况下，处于相同安全级别的接口之间不能通信，包不能在同一接口进出。允许相同安全级别的接口间通信，可以带来以下利益：

- 可以配置超过 101 个通信接口。如果每个接口都使用不同的安全级别，并且不将任何接口指派至相同安全级别，那么，每个安全级别（0～100）只能配置一个接口。
- 无需访问列表就能够在所有相同安全级别的接口之间进行通信。即使启用了相同级别安全接口通信，也仍然可以为接口配置不同的安全级别。

启用相同安全级别的接口，使其相互之间可以通信。

```
same-security-traffic permit inter-interface
```

内置接口通信被用于 VPN 通信的入口，并在同一接口路由出站。在这种情况下，VPN 通信既可以不加密，也可以为另一个 VPN 连接重新加密。

启用主机与同一接口连接之间的通信。

```
same-security-traffic permit intra-interface
```

18.3.8 配置桥组

1. 桥组配置策略

在透明模式下配置桥组时，应当遵循以下策略：

- 无论是单一模式，还是多环境模式中的每个环境，最多可以配置 8 个桥组。必须使用至少一个桥组，数据接口必须属于一个桥组。

> **提示** 尽管在 ASA 5505 上可以配置多个桥组，但是，在透明模式下，限定只能有 2 个数据接口，这意味着只能有效使用一个桥组。

- 每个桥组最多可以容纳 4 个接口。
- 每个桥组都需要一个管理IP地址，以实现相互之间的管理通信以及通过ASA的通信。与路由模式每个接口都需要一个 IP 地址不同，透明防火墙将一个 IP 地址指派给全部桥组。在发起包的 ASA 上，使用该 IP 地址作为源地址，如系统管理或 AAA 通信。除了桥组管理地址之外，还可以根据需要为一些模块配置管理接口。管理 IP 地址必须与所连接的网络处于同一子网。不能将子网设置为一个主机子网（255.255.255.255）。ASA 只有与管理 IP 地址处于同一网络才能通信。
- 在多环境模式下，每个虚拟防火墙必须使用不同接口，不能跨越环境共享接口。
- 在多环境模式下，每个虚拟防火墙通常都使用不同的子网。当然，也可以使用重叠的子网，但是，网络拓扑需要路由和 NAT 配置，以使其从路由的角度来看成为可能。

2. 桥组配置步骤

① 创建一个桥组，*bridge_group_number* 取值范围为 1～100。

```
hostname(config)# interface bvi bridge_group_number
```

② 为该桥组指定管理 IP 地址。不能为桥组指定主机地址（/32 或 255.255.255.255）。另外，也不能使用其他少于 3 个主机地址（包括上连路由、下连路由和透明防火墙）的子网（/30 或 255.255.255.252）。ASA 丢弃所有来自（或发往）子网第一个（或最后一个）地址的 ARP 包。因此，如果使用/30 子网，并为从该子网至上连路由指定一个预留地址，那么，ASA 将丢弃从下行路由至上行路由的 ARP 请求。Standby 关键字和地址用于失效备援。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

18.3.9 监视接口

显示接口统计信息。

```
show interface
```

显示接口 IP 地址和状态。

```
show interface ip brief
```

显示 EtherChannel 的 LACP 信息，如传输统计信息，系统标识和邻接详细信息。

```
show lacp {[channel_group_number] {counters| internal | neighbor} | sys-id}
```

显示 EtherChannel 信息，输出为详细信息和单行汇总。该命令也显示端口和端口汇聚的相关消息。

```
show port-channel [channel_group_number] [brief | detail | port | protocol | summary]
```

18.4 配置 DNS 和 DHCP

18.4.1 配置 DNS

一些 ASA 功能需要配置 DNS 服务器，以便借助域名访问外部服务器，例如，Botnet Traffic Filter（僵尸网络过滤）功能需要 DNS 服务器访问动态数据库服务，并在静态数据库中解决这些条目。另外，如 ping 或 traceroute 命令，可以输入欲 ping 或追踪路由的名称，ASA 就可以通过与 DNS 服务器通信来解析名称。许多 SSL VPN 和证书命令也支持名称。

① 使 ASA 能够向 DNS 服务器发送 DNS 请求，以实现名称解析。

```
hostname(config)# dns domain-lookup interface_name
```

② 指定 ASA 用于发出请求的 DNS 服务器组。

```
hostname(config)# dns server-group DefaultDNS
```

③ 指定一个或多个 DNS 服务器。既在同一命令中可以输入 6 个 IP 地址，彼此之间使用空格分隔，也可以分别使用命令一一指定。ASA 将顺序尝试每个 DNS 服务器，直至接收到应答为止。

```
hostname(config)# name-server ip_address [ip_address2] [...] [ip_address6]
```

可以使用 show dns-hosts 命令查看 DNS 缓存。其中，既包括从 DNS 服务器动态学习的条目，也包括使用 name 命令手工添加的名称和 IP 地址。

```
show dns-hosts
```

18.4.2 配置 DHCP

DHCP 服务器为网络客户端提供网络配置参数，如 IP 地址信息。ASA 可以为 DHCP 客户端提供一个 DHCP 服务器或 DHCP 中继服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。DHCP 中继需要在一个接口接受请求，并将其发送至使用另一个接口的外部 DHCP 服务器。

1. DHCP 配置策略和限制

在配置 DHCP 服务器和中继时，应当遵循以下配置策略和限制：

- 在 ASA 的每个接口上都可以配置 DHCP 服务器，每个接口都可以有自己的地址池。不过，其他 DHCP 设置，如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器，则在所有接口配置和使用。
- 如果一个接口已经启用了 DHCP 服务，那么，就不能在该接口上再配置 DHCP 客户端或 DHCP 中继。另外，DHCP 客户端必须直接连接至已经启用 DHCP 服务的接口。

- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务器同时使用。
- 如果已经启用了 DHCP 服务器，那么，中继代理就不能再启用。
- 当接收到一个 DHCP 请求时，ASA 将向 DHCP 服务器发送一个发现消息。该消息包括在组策略中使用 dhcp-network-scope 命令配置的 IP 地址（一个子网内）。如果服务器有地址池，并在该子网内，服务器将向该 IP 地址，而不是发现消息的 IP 地址发送池应答消息。
- 支持 Active/Active 和 Active/Standby 失效备援。
- 支持路由和防火墙模式。
- 支持单一模式和多环境模式。

2. 配置 DHCP 服务器

DHCP 服务器配置过程如下：

① 建立一个 DHCP 地址池。ASA 从地址池中为每个客户端分配一个 IP 地址使用。这些地址在本地，是直接连接到网络的非转换地址。地址池必须与 ASA 接口位于同一子网。

```
hostname(config)# dhcpd address ip_address-ip_address interface_name
```

② （可选）指定 DNS 服务器的 IP 地址。

```
hostname(config)# dhcpd dns dns1 [dns2]
```

③ （可选）指定 WINS 服务器的 IP 地址。

```
hostname(config)# dhcpd wins wins1 [wins2]
```

④ （可选）修改客户端租约时间。所谓租约时间，是指在租约期满之前，客户端可以使用所分配 IP 地址的时间（秒）。取值范围为 0～1 048 575，默认为 3600 s。0 为无限期租约。

```
hostname(config)# dhcpd lease lease_length
```

⑤ （可选）配置域名。

```
hostname(config)# dhcpd domain domain_name
```

⑥ （可选）配置 DHCP ping 超时值。为避免地址冲突，在为 DHCP 客户端分配地址之前，ASA 先发送 2 个 ICMP ping 包到该地址。该命令用于指定这些包的超时值。

```
hostname(config)# dhcpd ping_timeout milliseconds
```

⑦ 定义发送至 DHCP 客户端的默认网关。如果不使用 dhcpd option 3 命令定义默认网关，DHCP 客户端将使用管理接口的 IP 地址作为默认网关，将导致 DHCP ACK 不包括该选项。管理接口不能路由通信。

```
hostname(config)# dhcpd option 3 ip gateway_ip
```

⑧ 启用 DHCP 守护进程，在启用 DHCP 服务的接口上侦听 DHCP 客户端请求。

```
hostname(config)# dhcpd enable interface_name
```

3. 配置 DHCP 中继服务

DHCP 中继代理允许 ASA 将来自客户端的 DHCP 请求转发至连接在不同端口上的路由器。在配置 DHCP 中继代理时，应当遵循以下规定：

- 如果已经启用 DHCP 服务器，那么，就不能再启用中继代理。
- DHCP 客户端必须直接连接至 ASA，不能通过另一个中继代理或跌幅器发送请求。
- 在多环境模式下，不能在由多个环境使用的接口上启用 DHCP 中继。
- 在透明防火墙模式下，DHCP 中继服务不可用。处于透明防火墙模式的 ASA 只允许 ARP 通信通过，除此之外的其他所有通信都需要使用访问列表。若欲允许 DHCP 请求和应用通过透明模式的 ASA，需要配置 2 个访问列表，一个允许 DHCP 请求从内部接口向外部接口，一个允许应答从服务器进入到其他方向。
- 当 DHCP 中继被启用，并且多于一个 DHCP 中继服务被定义时，ASA 将把客户端请求转发至每个定义的 DHCP 中继服务。来自服务器的应答也被转发至客户端，直至客户端 DHCP 中继捆绑被移除。只有当 ASA 接收到 ACK、NACK 或拒绝等 DHCP 消息时，捆绑才将被移除。

> **提·示** 不能在运行 DHCP 代理服务器的接口上启用 DHCP 中继。必须先移除 VPN DHCP 配置，否则，将得到一条错误消息。

DHCP 中继的具体配置过程如下：

① 设置 DHCP 服务器的 IP 地址。DHCP 服务器与 DHCP 客户端在不同的接口上。可以使用该命令 10 次以标识最多 10 个服务器。

```
hostname(config)# dhcprelay server ip_address if_name
```

② 在连接客户端的接口上启用 DHCP 中继。

```
hostname(config)# dhcprelay enable interface
```

③ （可选）设置允许转达地址协商的时间（s）。

```
hostname(config)# dhcprelay timeout seconds
```

④ （可选）修改包中从 DHCP 服务器到 ASA 接口的第一个默认路由地址。其作用是允许客户端设置自己的默认路由，即使 DHCP 服务器已经指定了不同的路由器。

```
hostname(config)# dhcprelay setroute interface_name
```

4. 监视 DHCP

查看当前的 DHCP 配置。

```
show running-config dhcpd
```

查看当前的 DHCP 中继服务状态。

```
show running-config dhcprelay
```

18.5　配置对象和访问列表

对象是配置中可以重复使用的要素，可以在 ASA 配置中包含 IP 地址的部分定义和使用。借助对象，可以让配置变得更加简单，因为只需在一处修改对象，即可在引用它的所有位置都反映出来。如果没有对象，那么，就需要逐一修改这些参数功能，而不能一次搞定。例如，一个网络对象定义了一个 IP 地址和子网掩码，如果想改变 IP 地址，只需简单地在对象定义中修改它即可，而不必在引用它的每个功能中逐一进行修改。

18.5.1　配置对象和组

ASA 支持对象和对象组。根据需要，可以将对象添加至一个或多个对象组，或者将对象从对象组移除。

1.　对象和对象组简介

对象在包含有 IP 地址的配置中创建和使用。可以使用 IP 地址和子网掩码对或协议定义对象，并将其用于各自的配置中。无论何时，当需要修改 IP 地址或协议时，将不必再修改运行配置中的所有规则，只是简单地修改对象，就能够将修改自动应用于所有使用该对象的规则。在 Cisco ASA 中可以配置两种类型的对象，即网络对象和服务对象，都能应用于 NAT（Network Address Translation，网络地址转换），访问列表（Access List）和对象组。

对象组与对象类似，可以在 ACE 中使用对象组，而不必再分别输入每个对象。可以创建下列类型的对象组：

- 协议
- 网络
- 服务
- ICMP 类型

例如，可以考虑创建 3 个对象组：

- MyService——包含允许访问内部网络服务请求的 TCP 和 UDP 端口号。
- TrustedHosts——包含允许访问重要的服务和服务器的主机和网络地址。
- PublicServers——包含提供重要访问的服务器的主机地址。

在创建这些组之后，就可以仅用一个 ACE（Access Control Entry，访问控制项）来允许信任主机向组或公共服务器发出指定的服务请求。

2.　配置策略和限制

在配置对象和对象组时，应当遵循以下配置策略和限制：

- 对象和对象组支持单一和多模式环境模式。
- 对象和对象组支持路由和透明防火墙模式。
- 对象和对象组共享同一名称空间。
- 对象组必须有唯一的名称。
- 如果对象组正在命令中使用，那么，不能移除该对象组，或者使该对象组为空。

3. 配置网络对象

网络对象包含一个 IP 地址/子网掩码对。网络对象可以是三种类型，即主机、子网或范围。

① 创建一个新的网络对象。obj_name 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。提示符将切换到网络对象配置模式。

```
hostname(config)# object-network obj_name
```

② 将 IP 地址指定至该对象。可以配置主机地址、子网或地址范围。

```
hostname(config-network-object)# {host ip_addr | subnet net_addr net_mask |
range ip_addr_1 ip_addr_2}
```

③ 添加对该对象的描述。

```
hostname(config-network-object)# description text
```

4. 配置服务对象

服务对象包含协议、源和/或目的端口。

① 创建一个新的服务对象。obj_name 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。提示符将切换到服务对象配置模式。

```
hostname(config)# object-network obj_name
```

② 为源映射地址创建一个服务对象。Protocol 用于指定 IP 协议名称或数值。ICMP、TCP 或 UDP 关键字指定该服务对象是 ICMP、TCP 或 UDP 协议中的哪一个。Icmp-type 用于命名 ICMP 类型。Source 用于指定源端口。Destination 用于指定目的端口。Operator port 用于指定支持配置端口协议的端口/代码值。当以 TCP 或 UDP 配置端口时，可以指定“eq,”（等于）、“neq,”（不等于）、“lt,”（小于）、“gt,”（大于）和“range”（范围）。

```
hostname(config-service-object)# service {protocol | icmp icmp-type | {tcp |
udp} [source operator port] [destination operator port]}
```

5. 添加协议对象组

添加协议对象组之后，可以重复添加多个对象至同一组，并指定添加对象。

① 添加协议组，obj_grp_id 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。提示符将切换到协议配置模式。

```
hostname(config)# object-group protocol obj_grp_id
```

② （可选）添加描述，最多 200 个字符。

```
hostname(config-protocol)# description text
```

③ 在组中定义协议。每个协议都需要重复输入该命令。使用数值（1～254）或关键字（如 icmp,tcp 或 udp）标识指定的 IP 协议。常见协议数值如表 18-2 所示。如果是包含所有的 IP 协议，则使用关键字 ip。

```
hostname(config-protocol)# protocol-object protocol
```

表 18-2 常见协议数值表

协议	数值	描述
ah	51	Authentication Header（IPV6 认证头）
eigrp	88	Enhanced Interior Gateway Routing Protocol（增强内部网关路由协议）
esp	50	Encapsulated Security Payload（IPv6 封装安全载荷）
gre	47	Generic Routing Encapsulation（通用路由封装）
icmp	1	Internet Control Message Protocol（因特网控制消息协议）
icmp6	58	Internet Control Message Protocol（IPv6 因特网控制消息协议）
igmp	2	Internet Group Management Protocol（因特网组管理协议）
igrp	9	Interior Gateway Routing Protocol（内部网关路由协议）
ip	0	Internet Protocol（因特网协议）
ipinip	4	IP-in-IP encapsulation（IP-in-IP 封装）
ipsec	50	IP Security（因特网协议安全）
nos	94	Network Operating System（网络操作系统）
ospf	89	Open Shortest Path First（开放式最短路径优先路由协议）
pcp	108	Payload Compression Protocol（有效载荷压缩协议）
pim	103	Protocol Independent Multicast（协议无关组播）
pptp	47	Point-to-Point Tunneling Protocol（点对点隧道协议）
snp	109	Sitara Networks Protocol（Sitara 网络协议）
tcp	6	Transmission Control Protocol（传输控制协议）
udp	17	User Datagram Protocol（用户数据报协议）

6. 添加网络对象组

添加网络对象组之后，可以重复添加多个对象至同一组，并指定添加对象。

① 添加网络组，grp_id 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。提示符将切换到网络配置模式。

```
hostname(config)# object-group network grp_id
```

② （可选）添加描述，最多 200 个字符。

```
hostname(config-network)# description text
```

③ object 关键字用于将对象添加至网络对象组。

```
hostname(config-network)# network-object {object name | host ip_address |
ip_address mask}
```

7. 添加服务对象组

添加服务对象组之后，可以重复添加多个对象至同一组，并指定添加对象。

① 添加服务组，grp_id 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。为网络服务（即端口）指定协议时，需要使用 tcp,udp 或 tcp-udp 关键字。如果网络服务同时需要使用 TCP 和 UDP 同一端口号，则输入 tcp-udp 关键字（如 DNS 服务同时使用端口 53）。

```
hostname(config)# object-group service grp_id {tcp | udp |tcp-udp}
```

② （可选）添加描述，最多 200 个字符。

```
hostname(config-service)# description text
```

③ 定义组内端口。每个端口或端口范围都需要重复输入该命令。

```
hostname(config-service)# port-object {eq port | range begin_port end_port}
```

8. 嵌套对象组

可以分层嵌套对象组，以便在一个对象组中包括其他同一类型的对象组，并且混合和匹配嵌套组对象，使之在一个对象组中进行整合。若欲嵌套一个对象组至另一个同一类型的对象组，需要先创建欲嵌套的组，然后，再执行下述操作。

① 添加或编辑欲嵌套的对象组。grp_id 是一个最长 64 个字符的文本字符串，可以包括字母、数字、下画线“_”、连字符“-”或句号“.”。

```
hostname(config)# object-group group {{protocol | network |icmp-type} grp_id
|service grp_id {tcp |udp | tcp-udp}}
```

② 在上述对象组中，添加指定的对象组。嵌套组必须是相同类型，对象组可以混合和匹配嵌套组对象和规则对象。

```
hostname(config-network)# group-object group_id
```

9. 监视对象和组

显示访问列表项。

```
show access-list
```

显示当前所有对象组。

```
show running-config object-group
```

显示指定 ID 的对象组。

```
show running-config object-group grp_id
```

显示指定类型的对象组。

```
show running-config object-group grp_type
```

18.5.2 配置扩展访问列表

访问列表用于控制网络访问或指定传输。扩展访问列表由一条或多条访问控制项（Access Control Entries，ACE）组成，可以指定插入 ACE 的行号，源和目的地址，依赖 ACE 类型、协议，TCP 或 UDP 端口，或者 ICMP 类型。在 access-list 命令中可以确定所有这些参数，并且可以在所有参数中使用对象。

1. 配置策略和限制

在配置扩展访问列表时，应当遵循以下策略和限制：

- 在单一模式和多环境模式中均被支持。
- 在路由和透明防火墙模式中均被支持。
- 在配置中使用大写英文字母命名访问列表名称更容易被看到。访问列表既可以以接口命名（如 INSIDE），也可以用途来命名（如 NO_NAT 或 VPN）。
- 通常使用 ip 关键字来标识协议，当然，其他协议也是可以被接受的。

2. 添加扩展访问列表

访问列表由一个以上的 ACE 组成，创建访问列表由创建 ACE 并将之应用至列表开始。尽管列表中可以添加若干表项，但是，即使只有一个表项，也建议创建一个访问列表。

添加扩展 ACE。

用于 IP 通信，无端口。

```
access-list access_list_name [line line_number] extended {deny | permit}{protocol | object-group prot_grp_id} {source_address mask | object nw_obj_id | object-group nw_grp_id} {dest_address mask | object nw_obj_id | object-group nw_grp_id} [log [[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
```

用于 TCP 或 UDP 通信，有端口。

```
access-list access_list_name [line line_number] extended {deny | permit} {tcp | udp | object-group prot_grp_id} {source_address mask | object nw_obj_id | object-group nw_grp_id} [operator port | object-group svc_grp_id] {dest_address mask | object nw_obj_id | object-group nw_grp_id} [operator port | object-group svc_grp_id] [log [[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
```

用于 ICMP 通信。

```
access-list access_list_name [line line_number] extended {deny | permit} icmp {source_address mask | object nw_obj_id | object-group nw_grp_id} {dest_address mask | object nw_obj_id | object-group nw_grp_id} [icmp_type | object-group icmp_grp_id] [log [[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
```

其中，

line *line_number* 选项指定插入 ACE 的行号。如果不指定行号，ACE 将把该表项添加至列表最后。行号不会保存在配置中，只用于指定将该表项插入至 ACE 的哪个位置。

deny 关键字用于指明如果条件匹配则拒绝包，permit 关键字则用于指明如果条件匹配则允许包。

借助 object 或 object-group 关键字，可以在命令中使用网络对象、协议、网络、端口或 ICMP 对象组代替协议、IP 地址或端口。

protocol 用于指定 TCP/IP 协议的名称或数值，如 UDP 是 17，TCP 是 16，EGP 是 47，等等。

soure_address 用于指定发送包的网络或主机的 IP 地址。指定单一地址时，在 IP 地址前输入 host 关键字，而不是使用子网掩码。指定任意地址时，输入 any 关键字以代替地址和掩码。

对于 TCP 和 UDP 协议而言，*operator port* 选项用于匹配源或目的端口号。允许使用 lt（小于）、ge（大于）、dq（等于）、neq（不等于）和 range（范围）。当使用 range 时，只需指定起始端口号和终止端口号。

dest_address 用于指定接收包的网络或主机的 IP 地址。

如果协议为 ICMP 时，*icmp_type* 用于指定 ICMP 的类型。

time-range 关键字用于指定访问列表何时被激活。

inactive 关键字禁用 ACE。若欲重新启用，需要输入没有 inactive 关键字的 ACE。该功能用于保存非活动 ACE 的记录，以便在需要时进行恢复。

log 关键字用于记录日志。

例如，允许所有 IP 通信。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

3. 为访问列表添加备注

可以在扩展访问列表、EtherType 访问列表、标准访问列表和 Webtype 访问列表中添加关于表项的备注，从而使访问列表更容易查看、理解和排错。

在输入的访问列表之后，添加注释。text 最多可以包含 100 个字符。如果在所有 access-list 命令之前输入注释，该注释将作为访问列表的第一行。

```
access-list access_list_name remark text
```

若欲删除访问列表注释，可以使用 no access-list *access_list_name* 命令。

4. 监视扩展访问列表

显示访问列表表项。

```
show access list
```

显示当前运行访问列表配置。

```
show running-config access-list
```

5. 扩展访问列表配置示例

允许所有主机（应用该访问列表的接口上的）通过 ASA。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

阻止 192.168.1.0/24 网络中的主机对 211.82.218.0/27 网络访问，其余所有地址均被允许。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 
255.255.255.0 211.82.218.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

如果只想限制指定的主机，可以输入一个限制性的允许 ACE。默认情况下，除非明确允

许访问，否则，所有其他通信均被拒绝。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0 211.82.219.0 255.255.255.224
```

限制所有主机（在应用该访问列表的接口上）对Web站点（211.82.216.8）的访问，其他所有通信均被允许。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 211.82.216.8 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

使用对象组限制内部网络中的少量计算机访问少量Web服务器。其他通信均被允许。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

临时禁用允许从一个网络组对象（A）到另一个网络组对象（B）通信的访问列表。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

实施基于时间的访问列表，使用time-range命令定义指定时间。使用access-list extended命令将时间范围（Beijing_Minute）绑定至访问列表（Sales）。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 211.82.216.3 host 211.82.216.9 time-range Beijing_Minute
```

不使用对象组限制少量内部网络的计算机对少量Web服务器的访问，其他所有通信均被允许。

```
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.3 host 211.82.216.9 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.6 host 211.82.216.9 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.9 host 211.82.216.9 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.3 host 211.82.216.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.6 host 211.82.216.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.9 host 211.82.216.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.3 host 211.82.216.28 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.6 host 211.82.216.28 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 192.168.100.9 host 211.82.216.28 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

如果创建两个网络对象组，一个用于内部主机，一个用于 Web 服务器，那么，配置将变得更加简单，而且修改配置也变得更加容易。

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 192.168.100.3
hostname(config-network)# network-object host 192.168.100.6
hostname(config-network)# network-object host 192.168.100.9
hostname(config-network)# object-group network web
hostname(config-network)# network-object host 211.82.216.9
hostname(config-network)# network-object host 211.82.216.16
hostname(config-network)# network-object host 211.82.216.28
hostname(config-network)# access-list ACL_IN extended deny tcp port
object-group denied object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

18.5.3 配置 EtherType 访问列表

EtherType 访问列表由一条以上 ACE 构成，用于指定 EtherType。EtherType 规则借助 16 位十六进制数值控制 EtherType 标识，与控制其他类型的通信一样。配置 EtherType 访问列表分为两个步骤，即先通过添加 ACE 创建一个访问列表并为其指定名称，然后，再将访问列表应用至一个接口。

1. 配置策略和限制

配置 EtherType 访问列表，应当遵循以下策略和限制：

- 在单一模式和多环境模式下均有效。
- 只支持透明防火墙模式。
- 对 EtherType 访问列表而言，在列表最后时为隐示禁止，不影响 IP 传输或 ARP。例如，如果允许 EtherType 8037，在访问列表最后隐示拒绝，不会马上阻止任何事先在扩展访问表列中允许的 IP 通信（或者隐示允许从高安全接口至低安全接口）。不过，如果在 EtherType ACE 中明确拒绝了所有通信，那么 IP 和 ARP 通信将被禁止。
- 802.3 格式帧不会被访问列表操作，因为它们使用的长字段与字段类型有冲突。

2. 添加 EtherType 访问列表

添加一个 EtherType ACE。

```
access-list access_list_name ethertype {deny | permit} {ipx | bpdu | mpls-unicast
| mpls-multicast | is-is | any | hex_number}
```

其中，

access_list_name 用于指定访问列表的名称或号码。当指定访问列表名称时，ACE 添加至该访问列表最后。*access_list_name* 命名时最好采用大写字母，以便于在配置文件中查看和搜索。当然，也可以以应用该访问列表的接口（如 INSIDE）或目的（如 MPLS 或 PIX）作为访问列表的名称。

premit 关键字表明，如果条件匹配则允许访问。

deny 关键字表明，如果条件匹配则拒绝访问。如果 EtherType 访问列表配置为禁用所有通信，所有以太网帧将被丢弃。只有物理协议通信（如自协商）仍然被允许。

ipx 关键字指定访问 IPX。

bpdu 关键字指定访问 BPDU（Bridge Protocol Data Units，桥协议数据单元），默认为允许。

mpls-unicast 关键字指定访问 MPLS 单播。

mpls-multicast 关键字指定访问 MPLS 多播。

is-is 关键字指定访问 IS-IS 通信。

any 关键字指定访问任意通信。

hex_number 表示能够以大于或等于 0x600 十六进制数标识的 EtherType。

3. EtherType 访问列表配置示例

允许一些 EtherType 通过 ASA，只拒绝 IPX。

```
hostname(config)# access-list ETHER ethertype deny ipx
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

拒绝 EtherType 0x1256 通信，允许其他类型 EtherType 在两个接口间的通信。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

18.5.4 配置标准访问列表

标准访问列表用于标识 OSPF 路由的目的 IP 地址，并被用于 OSPF 重分布中的路由映射。标准访问列表不能被应用于接口以控制通信。

1. 配置策略和限制

配置标准访问列表，应当遵循以下策略和限制：

- 只支持单一环境模式。
- 支持路由模式和透明防火墙模式。
- 添加附加的 ACE 至访问列表末尾，输入另一个 access-list 命令，指定同一访问列表名称。
- 在使用 access-group 命令时，deny 关键字不允许包穿过 ASA。默认情况下，ASA 拒绝初始接口的所有包，除非指定了允许访问。
- 当指定了源、本地或目的地址，应用遵守下列规则。
  - 4 部分 32 位数，点分十进制。
  - 使用关键字 any 作为 IP 地址和子网掩码 0.0.0.0 0.0.0.0 的缩写。

  - 使用 host *ip_address* 选项作为子网掩码 255.255.255.255 的缩写。
- 可以在 access-list 命令中使用 inactive 关键字禁用 ACE。

2. 添加标准访问列表

添加标准访问列表项。若欲添加另一个 ACE 至访问列表末尾，可以使用 access-list 命令，并指定相同的访问列表名称。

```
hostname(config)# access-list access_list_name standard {deny | permit} {any
| ip_address mask}
```

其中，

access_list_name 用于指定访问列表的名称或号码。

any 关键字表示，访问其中的任何一个。

deny 关键字表示，如果条件匹配即拒绝访问。

permit 关键字表示，如果条件匹配即允许访问。

ip_address mask 表示访问指定的 IP 地址和子网掩码。

3. 标准访问列表配置示例

禁止 IP 通信通过 ASA。

```
hostname(config)# access-list 66 standard deny
```

如果条件匹配，允许 IP 通信通过 ASA。

```
hostname(config)# access-list 66 standard permit
```

指定目的地址。

```
hostname(config)# access-list 66 standard permit host 10.10.10.10
```

18.5.5 配置 Webtype 访问列表

将 Webtype 访问列表添加至配置时，可以过滤无客户端的 SSL VPN。

1. 配置策略和限制

配置 Webtype 访问列表，应当遵循以下策略和限制：

- 支持单一模式和多环境模式。
- 支持路由模式和透明防火墙模式。
- access-list webtype 命令被应用于配置无客户端 SSL VPN 的过滤。URL（Uniform Resoure Locator，统一资源定位符）的指定既可以完整的，也可以是部分的，可以包含服务器通配符，还可以指定端口。
- 有效的协议标识是 http, https, cifs, imap4, pop3 和 smtp。如果涉及任何 URL，那么，URL 也可以包含关键字 any。另外，如果涉及到 DNS 名称时，也可以使用“*”号。

2. 添加带 URL 字符串的 Webtype 访问列表

将访问列表添加至配置文件，实现对无客户端 SSL VPN 的过滤。

access-list *access_list_name* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]]

其中，

access_list_name 指定访问列表的名称和号码。

any 关键字指定所有的 URL。

deny 关键字表示，如果条件匹配将拒绝访问。

interval 选项指定产生系统日志消息 106100 的时间间隔，取值范围为 1～600s。

log[[disable | default] | *level*]选项指定由 ACE 产生的系统日志消息 106100。当 log 选项关键字被指定时，系统日志消息 106100 的默认级别为 6（报告）。

permit 关键字表示，如果条件匹配将允许访问。

time_range *name* 选项指定一个附加 time-range 选项的关键字至访问列表。

url 关键字指定用于过滤的 URL。

url_string 选项用于指定被过滤的 URL。

在 Webtype 访问列表项中可以使用通配符。其中，“*”用于匹配无字符或字符中的任意数字；“?”用于精确匹配任意一个字符；“[]”用于匹配指定范围内的任意一个字符。

3. 添加带 IP 地址的 Webtype 访问列表

添加带 IP 地址的 Webtype 访问列表执行下述命令。

access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port*[*port*]] [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]]

其中，*access_list_name* 用于指定访问列表的名称或号码。

any 关键字指定所有 IP 地址。

deny 关键字表示，如果条件匹配将拒绝访问。

host *ip_address* 选项指定一个主机的 IP 地址。

interval 选项指定产生系统消息 106100 的时间间隔。有效取值范围为 1～600s。

ip_address ip_mask 选项指定 IP 地址和子网掩码。

log [[disable | default]| *level*]选项指定由 ACE 产生的系统日志消息 106100。当 log 选项关键字指定时，系统消息 106100 的默认级别为 6（报告）。

permit 关键字表示，如果条件匹配将允许访问。

port 选项指定 TCP 或 UDP 端口的名称或代码。

time_range *name* 选项指定一个附加 time-range 选项的关键字至访问列表。

4. Webtype 访问列表配置示例

禁止对指定 URL 的访问。

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

禁止访问指定的文件。

```
hostname(config)# access-list acl_file webtype deny url https:// www.example.com/
dir/file.html
```

禁止 HTTP 访问至任何 URL 地址的 8080 端口。

```
hostname(config)# access-list acl_company webtype deny url http://
my-server:8080/*
```

使用通配符匹配 URL，如 http://www.example.com/和 http://www.example.net/。

```
access-list test webtype permit url http://www.**ample/
```

使用通配符匹配 URL，如 http://www.cisco.com 和 ftp://wwz.example.com。

```
access-list test webtype permit url *://ww?.c*co*/
```

使用通配符匹配 URL，如 http://www.cisco.com:80 和 https://www.cisco.com:81。

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

使用通配符匹配 URL，如 http://www.example.com 和 http://www.example.net。

```
access-list test webtype permit url http://www.[a-z]ample?*/
```

18.5.6 配置访问列表日志

默认情况下，当通信被扩展 ACE 或 Webtype ACE 拒绝时，ASA 将会为每个拒绝包都产生一个系统日志消息 106023，内容大致如下：

```
%ASA|PIX-4-106023: Deny protocol src [interface_name:source_address/ source_port]
dst
interface_name:dest_address/dest_port [type {string}, code {code}] by access_group
acl_id
```

如果 ASA 被攻击，被拒绝包的系统日志消息数量将会非常大。因此，推荐使用系统日志消息 106100 进行代替，为每个 ACE 提供统计信息，并启用系统日志数量限制。当然，作为选择之一，也可以禁用所有日志。

在扩展访问列表命令结尾的 log 选项，可以设置如下动作：

- 启用消息 106100 代替消息 106023。
- 禁用所有日志。
- 恢复默认日志，使用消息 106023。

系统日志消息 106100 使用下述结构：

```
%ASA|PIX-n-106100: access-list acl_id {permitted | denied} protocol
interface_name/source_address(source_port) -> interface_name/dest_address
(dest_port)
hit-cnt number ({first hit | number-second interval})
```

为 ACE 配置日志的命令格式如下：

```
access-list access_list_name [extended] {deny | permit}...[log [[level] [interval secs] | disable | default]]
```

其中，

access-list *access_list_name* 用于指定欲配置日志的访问列表。

extended 选项添加一个 ACE。

deny 关键字表示，如果条件匹配将拒绝包。一些功能不允许拒绝 ACE，如 NAT。

permit 关键字表示，如果条件匹配将允许包。

如果输入没有任何参数的 log 选项，将启用系统日志消息 106100，默认级别为 6，默认间隔为 300s。

level 表示严重级别，取值范围为 0～7，默认值为 6。

interval *secs* 表示两个系统日志消息之间的时间间隔，取值范围为 1～600，默认为 300。

disable 表示禁用所有访问列表日志。

default 表示启用日志消息 106023。该设置与没有 log 选项相同。

18.6 配置 NAT

IP 网络中的每一台计算机和设备都使用唯一的 IP 地址进行标识。由于 IPv4 地址的短缺，许多网络内部的计算机设备都使用私有 IP 地址，而私有 IP 地址是无法访问外部网络的。借助 NAT 技术，可以完美实现内部网络对 Internet 的访问。NAT 将私有 IP 地址替换为公有 IP 地址，在内部网络中转换私有 IP 地址，使其可路由并访问 Internet。

18.6.1 ASA 支持的 NAT 类型

Cisco ASA 可以采用以下方式实施 NAT。

- 静态 NAT（Static NAT）——真实 IP 地址和映射 IP 地址之间固定映射，允许双向发起通信。
- 动态 NAT（Dynamic NAT）——真实 IP 地址组被映射至一个映射 IP 地址组（通常很小），先到先得。只有真实主机可以发起通信。
- 动态端口地址转换（Dynamic Port Address Translation，PAT）——真实 IP 地址组使用唯一的源端口被映射至一个 IP 地址。
- Identity NAT——真实 IP 地址被静态转换为其自己，本质上来说，就是绕开 NAT。当想转换大组 IP 地址时，可以采用该方式来配置 NAT。

18.6.2 NAT 规则顺序

网络对象（Network Object）NAT 规则和 Twice NAT 规则被存储于一张表中，并被分为三个部分。第一部分规则首先应用，然后是第二部分，最后才是第三部分，如表 18-3 所示。

表 18-3 NAT 规则表

表中的部分	规则类型	每部分内部规则的顺序
第 1 部分	Twice NAT	在首次匹配的基础上应用，其顺序为在配置文件中出现的位置。默认情况下，Twice NAT 规则被添加至第 1 部分 如果配置了 EasyVPN 远程，ASA 动态添加隐式 NAT 规则至该部分的末尾。当然，不能在该部分配置 Twice NAT 规则以匹配 VPN 通信，而不是匹配隐式规则。如果由于 NAT 失败而导致 VPN 不能正确工作，应当考虑将 Twice NAT 规则添加至第 3 部分
第 2 部分	网络对象 NAT	第 2 部分规则由 ASA 自动按照下述顺序应用： ● 静态规则 ● 动态规则 在每个规则类型中，按照下述准则排序： ● 依据真实 IP 地址的数量，从小到大排序。例如，拥有 1 个地址的对象将排在拥有 10 地址的对象之前 ● 如果数量相同，那么，将按照 IP 地址号码从低到高排序。例如，10.1.1.0 将排在 11.1.1.0 之前 ● 如果使用 IP 地址相同，那么，将按照网络对象名称字母排序。例如，inside 将排在 outside 之前
第 3 部分	Twice NAT	第 3 部分规则在首次匹配的基础上应用，其顺序为在配置文件中出现的位置 当需要添加规则时，可以在第 3 部分添加 Twice NAT 规则

18.6.3 配置网络对象 NAT

所有配置为网络对象参数的 NAT 规则，被认为是网络对象 NAT 规则。网络对象 NAT 是为某个 IP 地址、某段 IP 地址或某个子网配置 NAT 的快捷方式。配置网络对象之后，接下来就是为该对象标识映射地址。

1. 配置策略和限制

在配置网络对象映射时，应当遵循以下策略和限制：

- 支持单一模式和多环境模式。
- 支持路由模式和透明防火墙模式。
- 在透明模式中，必须指定真实的接口和映射接口，不能使用 any。
- 在透明模式中，不能配置接口 PAT，因为透明模式接口没有 IP 地址。同时，也不能使用管理 IP 地址作为映射地址。
- 只能为特定的对象定义一个 NAT 规则。如果想为对象配置多个 NAT 规则，需要创建拥有不同名称的多个对象，并为其指定同一 IP 地址。如 object network obj-10.10.10.1-01，object network obj-10.10.10.1-02，等等。
- 如果想改变 NAT 配置，并且不想在新 NAT 配置使用前等待现有转换超时，可以使用 clear xlate 命令清除转换表。不过，清除转换表将断开当前所有用于转换的连接。

提·示

若欲移除动态 NAT 或 PAT 规则，然后添加带有映射地址的新规则，如果映射地址与移除规则中的地址相重叠，那么，新规则在所有与移除规则相联系的连接超时前将不能使用，当然，也可以使用 clear xtate 命令清除当前所有连接。该措施将确保同一地址不会被分配至多个主机。

- 用于 NAT 的对象和对象组必须是明确的，必须包含 IP 地址。
- 在多个 NAT 规则中，可以使用相同的映射对象或组。
- 映射 IP 地址池不能包含以下地址：
  - 映射接口地址。如果规则指定了 any 接口，所有接口 IP 地址都将不被允许。对于接口 PAT（仅限于路由模式）而言，可以使用 interface 关键字代替 IP 地址。
  - （透明模式）管理 IP 地址。
  - （动态 NAT）在启用 VPN 时，备用接口的 IP 地址。
  - VPN 地址池中已有的 IP 地址。

2. 配置动态 NAT

配置网络对象 NAT 为动态 NAT（Dynamic NAT），操作过程如下。

① 指定映射地址（即想转换的地址），配置网络对象或网络对象组。网络对象组可以包括对象和/或内联地址。如果映射网络对象同时包含 IP 地址范围和主机 IP 地址，那么，IP 地址范围将使用动态 NAT，主机 IP 地址则使用 PAT。

提·示

对象或对象组不能包含子网。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# range ip_address_1 ip_address_2
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | host
ip_address} | group-object grp_obj_name}
```

② 为 NAT 配置网络对象，或者，在已有网络对象时可进入对象网络配置模式。

```
hostname(config)# object network obj_name
```

③ 如果创建了新的网络对象，定义欲转换的真实 IP 地址。

```
hostname(config-network-object)# {host ip_address | subnet subnet_address
```

```
netmask | range ip_address_1 ip_address_2}
```

④ 为对象 IP 地址配置动态 NAT。其中，

Interface，（透明模式下必须）指定真实和映射接口，并确认命令行中使用了“()”。在路由模式中，如果没有指定真实和映射接口，所有接口都将被使用。也可以为一个或两个接口都指定关键词 any。

映射 IP 地址，指定映射 IP 地址为已经创建的网络对象或对象组。

接口 PAT 回退，（可选）Interface 关键字启用接口 PAT 回退。在映射 IP 地址启用后，映射接口的 IP 地址将被使用。对该选项而言，必须使用 *mapped_ifc* 配置指定接口（在透明模式中不能指定 interface）。

DNS，（可选）dns 关键字转换 DNS 应答。确认 DNS 检查为启用状态（默认为启用）。

```
hostname(config-network-object)# nat [(real_ifc,mapped_ifc)] dynamic mapped_obj [interface] [dns]
```

下述示例为配置动态 NAT，将 192.168.1.0 网络隐藏在外部地址 10.1.1.1 - 10.1.1.10 之后。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.1.1.1 10.1.1.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

下述示例为配置带有动态 PAT 备份的动态 NAT。内部网络 10.11.11.0 中的主机被映射 nat-range1 地址池（10.10.10.10 – 10.10.10.20）。nat-range1 地址池所有地址被分配完毕之后，动态 PAT 使用 pat-ip1 地址（10.10.10.21）。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20
hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21
hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1
hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.11.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

3. 配置动态 PAT（隐藏）

在配置动态 PAT（隐藏）时，应当遵循以下策略：

- 如果可用，直接源端口号将被用于映射端口。如果真实端口不可用，默认情况下，映射端口选择同一范围内的端口作为真实端口号，即 0～511、512～1023 和 1024～65535。可见，1024 端口以下将只有少量 PAT 池能够使用。因此，如果较低范围端口有大量的传输，那么，应该指定较大范围的端口，如 1024～65535，或者 1～65535。
- 如果在两个规则中使用同一 PAT 地址池对象，应当确认每个规则中使用了相同的选项。例如，一个规则指定了扩展 PAT 和一个宽范围，另一个规则也必须指定扩展 PAT

和一个宽范围。

- 许多应用程序检视不支持扩展 PAT。
- 如果为动态 PAT 规则启用扩展 PAT，不能使用 PAT 地址池中的地址作为静态 NAT-with-port-translation 规则中的 PAT 地址。例如，PAT 地址池包括 10.1.1.1，那么，就不能创建静态 NAT-with-port-translation 规则使用 10.1.1.1 作为 PAT 地址。
- 如果使用了 PAT 池，并且指定了回退接口，就不能再指定扩展 PAT。
- 如果主机已经拥有连接，那么，后续的每个连接都可能使用不同的 PAT 地址。

配置过程如下：

① （可选）指定映射地址（即欲转换为的地址）。可以配置一个地址、一个 PAT 池或者多个地址。配置一个网络对象或网络对象组。网络对象组可以包含对象和/或内联地址。作为选择，如果只想在 nat 命令中使用一个 IP 地址，或者通过指定 interface 关键字使用接口地址，也可以跳过该步骤。映射地址用于 PAT 池，对象或组中的所有地址都被用于 PAT 地址。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | host ip_address} | group-object grp_obj_name}
```

② 为 NAT 配置网络对象，或者在已有的网络对象中进入对象网络配置模式。

```
hostname(config)# object network obj_name
```

③ 如果创建一个新网络对象，定义欲转换的真实 IP 地址。

```
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

④ 配置动态 PAT。每个对象只能定义一个 NAT 规则。

```
hostname(config-network-object)# nat [(real_ifc,mapped_ifc)] dynamic {mapped_inline_host_ip | mapped_obj | pat-pool mapped_obj [round-robin] [extended] [flat [include-reserve]] | interface} [interface] [dns]
```

其中，

- 接口（Interface），（透明模式所必需）指定真实和映射接口。确认在命令中包括“()”。在路由模式中，如果不指定真实和映射接口，所有接口都将被使用。可以在一个或两个接口都使用关键字 any。
- 映射 IP 地址（Mapped IP Address），可以指定映射 IP 地址为：
  - 内联主机地址。
  - 定义为主机地址的已有网络对象。
  - pat-pool，包含有多个地址的已有网络对象或组。

- interface，（只适用于路由模式）映射接口的 IP 地址被用于映射地址。对该选项而言，必须为 mapped_ifc 配置指定接口。若欲使用接口 IP 地址，必须使用该关键字。
- PAT 池，可以指定一个或多个下列选项：
  - 循环（Ronnd Robin），round-robin 关键字为 PAT 池启用 round-robin 地址分配。如果不使用循环，那么，默认情况下，在下一个 PAT 地址使用之前，所有 PAT 地址的端口都将被分配。round-robin 在再次重新使用第一个地址之前，将从池中为每个 PAT 地址指派一个地址/端口，然后是第二个地址，等等。
  - 扩展 PAT（Extended PAT），extended 关键字启用扩展 PAT。扩展 PAT 的每个服务使用 65535 个端口。扩展 PAT 在转换信息中可以包含目的地址和端口。不过，一般情况下，创建 PAT 转换时，目的端口和地址将不被考虑，因此，每个 PAT 地址被限制为 65535 个端口。
  - 扁平范围（Flat Range），在分配端口时，flat 关键字将启用全部 1024～65535 端口范围。在选择转换使用的映射端口号时，ASA 使用有效的真实源端口号。然而，如果不使用该选项，如果真实端口无效，默认情况下，映射端口将选择同一范围（1～511，512～1023，1024～65535）的端口作为真实端口。为避免低范围端口用尽，应当配置该选项。若欲使用全部范围的 1～65535，也可以指定 include-reserve 关键字。
- 接口 PAT 回退（Interface PAT Fallback），（可选）在主要 PAT 地址之后，使用 interface 关键字可以启用接口 PAT 回退。当主要 PAT 地址启用后，映射接口的 IP 地址将被使用。若欲使用该选项，必须配置以 mapped_ifc 指定接口（不能在透明模式中指定接口 interface）。
- DNS，（可选）DNS 关键字转换 DNS 应答。确认已经启用 DNS 检视（默认被启用）。

例如，配置动态 PAT，将 192.168.1.0 网络隐藏在 10.1.1.1 之后。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.1.1.1
```

例如，配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口之后。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

4. 配置静态 NAT

配置静态 NAT（Static NAT）或带端口转换的静态 NAT（Static NAT-with-Port-Translation）的操作过程如下。

① 指定映射地址（即欲转换的地址），配置网络对象或网络对象组。网络对象组可以包含对象和/或内联地址。当然，若欲在 nat 命令中直接输入 IP 地址，或者借助 interface 关键字使用接口 IP 地址（适用于带端口转换的静态 NAT），也可以跳过该步骤。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

② 为 NAT 配置网络对象，或者如果已创建网络对象，则进入对象网络配置模式。

```
hostname(config)# object network obj_name
```

③ 如果创建一个新的网络对象，定义欲转换的真实 IP 地址。

```
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

④ 配置静态 NAT。

```
hostname(config-network-object)# nat [(real_ifc,mapped_ifc)] static {mapped_inline_ip | mapped_obj | interface} [dns | service {tcp | udp} real_port mapped_port] [no-proxy-arp]
```

其中，

- 接口（Interface），（透明模式所必需）指定真实和映射接口。确认在命令中包括“()”。在路由模式中，如果不指定真实和映射接口，所有接口都将被使用。可以在一个或两个接口都使用关键字 any。
- 映射 IP 地址（Mapped IP Address），可以指定映射 IP 地址为：
  - 内联 IP 地址。映射网络的子网掩码或范围与真实网络相同。例如，如果真实网络是主机，那么，该地址也将是主机地址。如果是多台主机，那么映射地址应当包含与真实范围相同数量的地址。例如，如果真实地址定义的范围为 10.1.1.1～10.1.1.6，并且指定 172.16.1.1 作为映射地址，那么，映射范围将包含 172.16.1.1～172.16.1.6。
  - 已有网络对象或组。
  - interface，（静态端口转换 NAT，路由模式）映射接口的 IP 地址被用于映射地址。对该选项而言，必须为 mapped_ifc 配置指定接口。若欲使用接口 IP 地址时，必须使用 service 关键字。
- DNS，（可选）DNS 关键字转换 DNS 应答。确认已经启用 DNS 检视（默认被启用）。
- 端口转换，（只适用静态端口转换 NAT）指定 tcp 或 udp，以及真实和映射端口。可以输入端口号或已知端口名称（如 ftp）。
- No Proxy ARP，（可选）指定 no-proxy-arp 关键字，使进入映射 IP 地址的包禁用 ARP 代理。

配置示例，为内部接口上的真实主机 10.1.1.1 至外部接口 10.2.2.2 配置静态 NAT，并启用 DNS 重写。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

使用映射对象，为内部接口上的真实主机 10.1.1.1 至外部接口 10.2.2.2 配置静态 NAT。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2
hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

为 10.1.1.1 的 T CP 端口 21 至外部接口 2121 端口配置静态端口转换 NAT。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service
tcp 21 2121
```

5. 配置 Identity NAT

使用网络对象配置 Identity NAT 的操作过程如下。

① （可选）为映射地址（与真实地址相同）配置网络对象。如果在 nat 命令中指定了 IP 地址作为内联，也可以跳过该步骤。

```
hostname(config)#object network obj_name
hostname(config-network-object)#{host ip_address | subnet subnet_address
netmask | range ip_address_1 ip_address_2}
```

② 为 Identity NAT 配置网络对象，或者如果已有的网络对象，则进入对象网络配置模式。

```
hostname(config)# object network obj_name
```

③ 如果创建了新的网络对象，定义欲执行 Identity NAT 的真实地址。如果在第 1 步为映射地址配置了网络对象，那么，这些地址必须相匹配。

```
hostname(config-network-object)#{host ip_address | subnet subnet_address
netmask | range ip_address_1 ip_address_2}
```

④ 配置 Identity NAT。

```
hostname(config-network-object)# nat [(real_ifc,mapped_ifc)] static {mapped_
inline_ip | mapped_obj} [no-proxy-arp] [route-lookup]
```

其中，

- 接口（Interface），（透明模式所必需）指定真实和映射接口。确认在命令中包括“()”。在路由模式中，如果不指定真实和映射接口，所有接口都将被使用。可以在一个或两个接口都使用关键字 any。
- 映射 IP 地址（Mapped IP Address），确认映射地址和真实地址配置为相同的 IP 地址。可以指定映射 IP 地址为：
  - ➢ 网络对象。与真实对象包含相同的 IP 地址。

- 内联 IP 地址。映射网络的子网掩码或范围与真实网络相同。例如，如果真实网络是主机，那么，该地址也将是主机地址。如果是多台主机，那么映射地址应当包含与真实范围相同数量的地址。例如，如果真实地址定义的范围为 10.1.1.1～10.1.1.6，并且指定 10.1.1.1 作为映射地址，那么，映射范围将包含 10.1.1.1～10.1.1.6。

- No Proxy ARP，（可选）指定 no-proxy-arp 关键字，使进入映射 IP 地址的包禁用 ARP 代理。
- Route 查找，（只适用于路由模式，指定接口）由 route-lookup 确定出口接口，使用路由查找代替 NAT 命令中指定的接口。

例如，使用内联映射地址映射主机地址至自己。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

再如，使用网络对象映射主机地址至自己。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1
-identity
```

6. 监视网络对象 NAT

查看 NAT 统计数据，包括每个 NAT 规则的次数。

```
show nat
```

查看 NAT 池统计数据，包括地址和端口分配，以及在不同时间是如何分配的。

```
show nat pool
```

查看 NAT 配置。

```
show running-config nat
```

7. 网络对象 NAT 配置示例

■ 访问内部的 Web 服务器（静态 NAT）

为内部 Web 服务器配置静态 NAT。真实地址是一个私有网络（10.1.1.0），公共地址也是必须的（211.82.216.0）。静态 NAT 可以强制主机发起至 Web 服务器（拥有固定地址）的通信（如图 18-4 所示）。

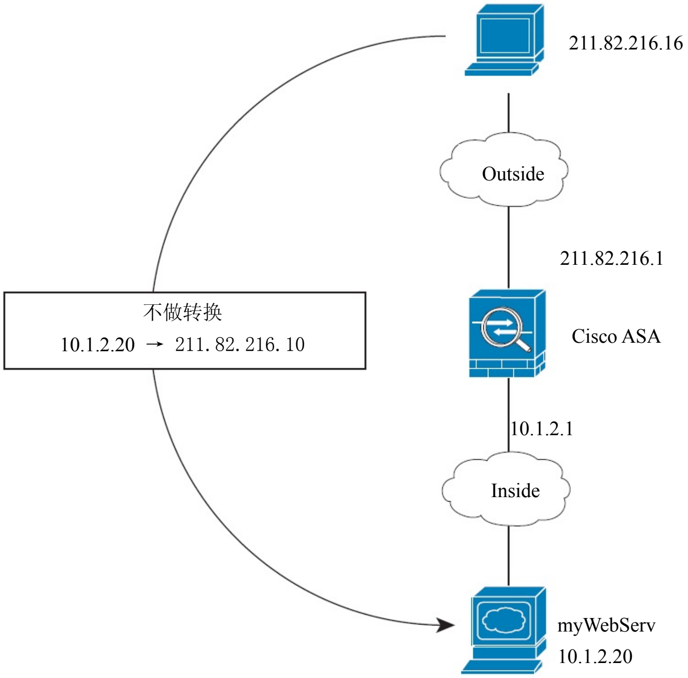


图 18-4　为访问内部 Web 服务器配置静态 NAT

配置过程如下：

① 为内部 Web 服务器创建一个网络对象。

```
hostname(config)# object network myWebServ
```

② 定义 Web 服务器的 IP 地址。

```
hostname(config-network-object)# host 10.1.2.20
```

③ 为该对象配置静态 NAT。

```
hostname(config-network-object)# nat (inside,outside) static 211.82.216.10
```

■　**为内部主机配置动态 NAT，为外部 Web 服务器配置静态 NAT**

当需要访问外部网络时，为私有网络上的内部用户配置动态 NAT。同时，当内部用户连接至外部 Web 服务器时，Web 服务器地址被转换为一个地址，就像在内部网络一样（如图 18-5 所示）。

配置过程如下：

① 为动态 NAT 池创建一个网络对象，用于转换内部地址。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 211.82.216.20 211.82.216.30
```

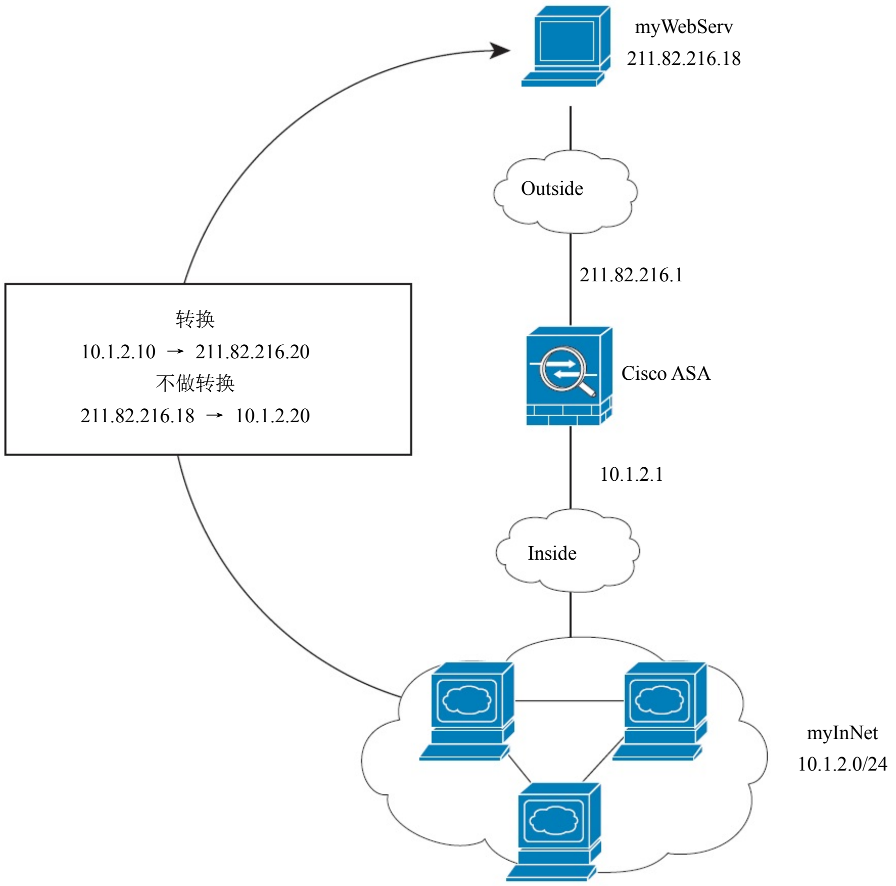


图 18-5　为内部主机配置动态 NAT，为外部 Web 服务器配置静态 NAT

② 为内部网络创建一个网络对象。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

③ 在内部网络启用动态 NAT。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

④ 为外部 Web 服务器创建一个网络对象。

```
hostname(config)# object network myWebServ
```

⑤ 定义 Web 服务器的 IP 地址。

```
hostname(config-network-object)# host 211.82.216.18
```

⑥ 为 Web 服务器配置静态 NAT。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

■ **借助多个映射地址实现内部负载均衡**

将内部网络负载均衡分配至多个 IP 地址。当外部主机访问一个映射 IP 地址时，不是转换至单个负载均衡地址，而是借助 URL 的请求，将通信转发至恰当的 Web 服务器（如图 18-6 所示）。

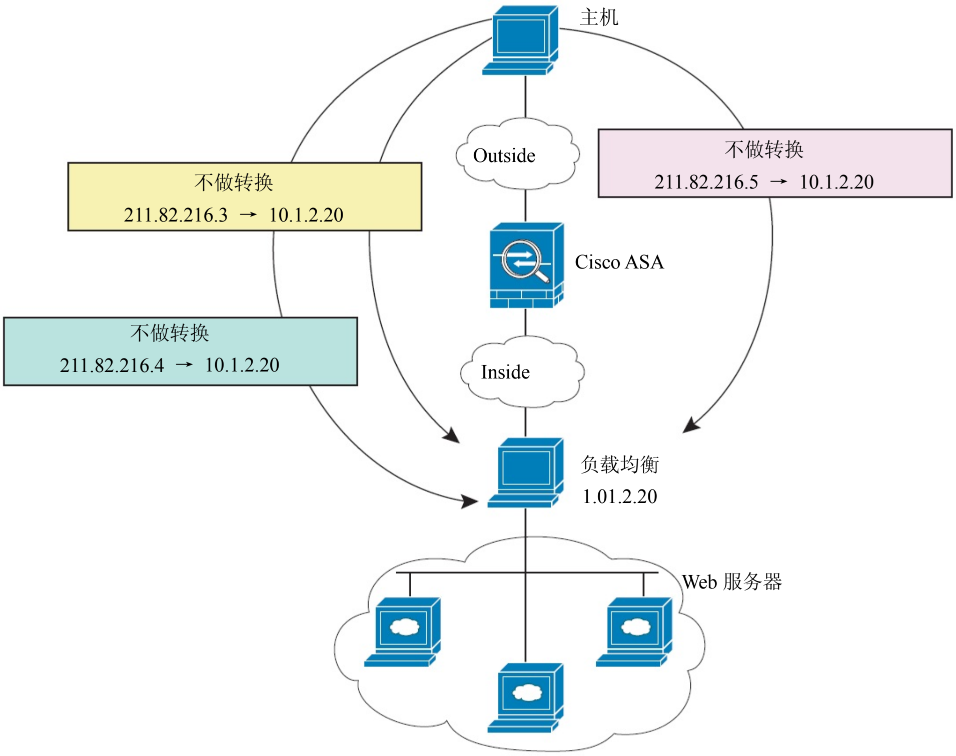


图 18-6　一对多静态 NAT 实现内部负载均衡

配置过程如下：

① 为欲映射负载均衡的地址创建一个网络对象。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 211.82.216.3 211.82.216.8
```

② 为负载均衡创建一个网络对象。

```
hostname(config)# object network myLBHost
```

③ 定义负载均衡地址。

```
hostname(config-network-object)# host 10.1.2.20
```

④ 为负载均衡配置静态 NAT。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

■ **FTP、HTTP 和 SMTP 使用一个 IP 地址**

借助静态端口转换 NAT，只使用一个 IP 地址，即可使远程用户访问 FTP、HTTP 和 SMTP

服务。这些服务器实际上分布在真实网络的不同设备上，但是，每个服务器都可以通过指定静态端口转换 NAT 规则来使用同一映射 IP 地址的不同端口（如图 18-7 所示）。

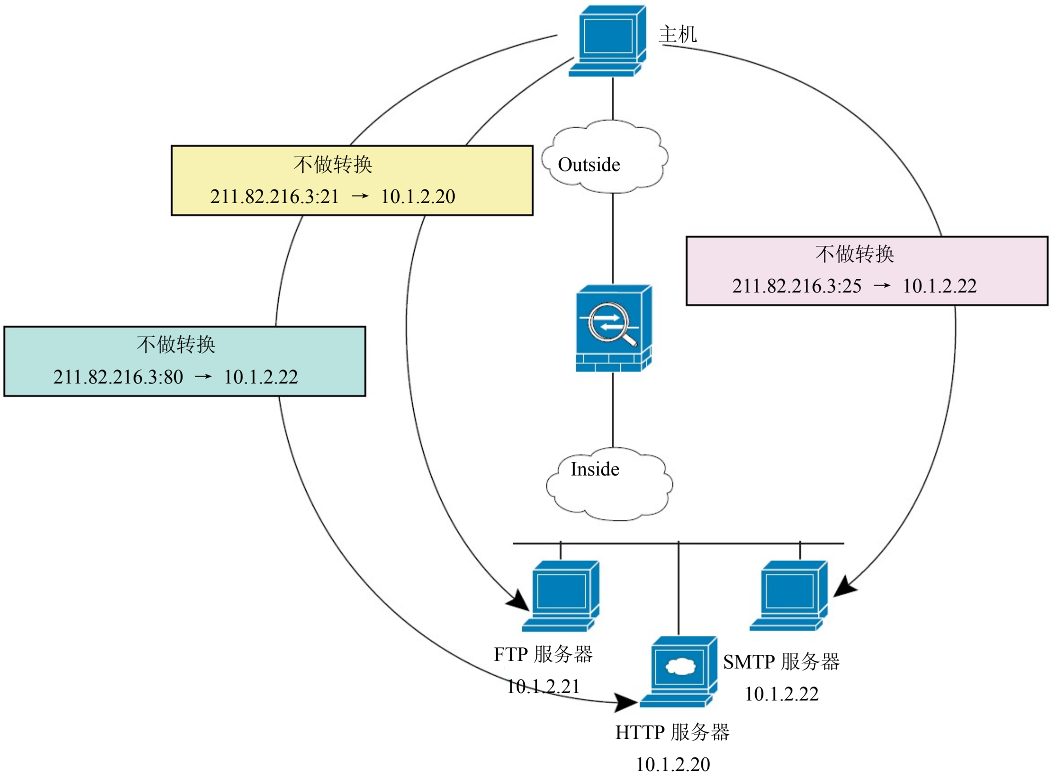


图 18-7　FTP、HTTP 和 SMTP 使用一个 IP 地址

① 为 FTP 服务器地址创建一个网络对象。

```
hostname(config)# object network FTP_SERVER
```

② 定义 FTP 服务器地址，并且配置标识 FTP 服务端口转换的静态 NAT。

```
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3
service tcp ftp ftp
```

③ 为 HTTP 服务器地址创建一个网络对象。

```
hostname(config)# object network HTTP_SERVER
```

④ 定义 HTTP 服务器地址，并且配置标识 HTTP 服务端口转换的静态 NAT。

```
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3
service tcp http http
```

⑤ 为 SMTP 服务器地址创建一个网络对象。

```
hostname(config)# object network SMTP_SERVER
```

⑥ 定义 SMTP 服务器地址，并且配置标识 SMTP 服务端口转换的静态 NAT。

```
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3
service tcp smtp smtp
```

18.6.4 配置 Twice NAT

Twice NAT 可以在一条规则中同时确定源和目的地址。同时指定源和目的地址的意义在于，指定一个源地址，使之在发往目的 X 时转换为 A，在发往目的 Y 时转换为 B。

Twice NAT 是 NAT 的一个变种，同时修改源和目的地址。这与传统 NAT 和双向 NAT 都不相同，传统 NAT 和双向 NAT 只翻译源或者目的地址（端口）。两次 NAT 在内部 IP 地址与外部 IP 存在冲突时非常有用。例如，当一个站点不恰当地使用了已分配给其他机构的公用 IP 地址时，或者，当一个站点从一家运营商换到另外一家运营商，并且希望在内部保留前一家运营商分配的地址（因为前一家运营商可能会在一段时间后将这些地址重新分配给其他主机使用），在这些情况下，外部网络的主机可能会分配到以前已分配给内部主机的同一地址。假如该地址出现在某个包中时，那么，应该将其转发给内部主机，而不是通过 NAT 转发给外部网络。Twice NAT 通过同时转换 IP 包的源和目的地址，解决了地址冲突的问题。

提·示

对于静态 NAT，规则是双向的，可以在命令和描述中查看到使用的源和目的地址。例如，配置端口地址转换 NAT 时，指定源地址为 Telnet 服务器，并且想让所有与 Telnet 服务器的通信都使用端口转换（从端口 2323 至端口 23），那么，必须指定源端口转换（真实 23，映射 2323）。之所以指定该源端口，是因为指定的 Telnet 服务器地址为源地址。

Twice NAT 的目的地址不是必须要配置的。若欲指定目的地址，既可以映射至自身（Identity NAT），也可以映射至不同地址。目的映射通常为静态映射。

在配置带端口转换的静态接口 NAT（NAT-with-Port-Translation）时，Twice NAT 也可以使用服务对象。网络对象 NAT 只在内联时适用。

1. 配置策略和限制

在配置 Twice NAT 时，应当遵循以下配置策略和限制。

- 真实和映射地址均可配置为网络对象或网络对象组（object network 或 object-group network 命令）。网络对象组特别适用于创建映射地址池（不相连的 IP 地址范围、多个主机或子网）。
- 带端口转换的静态接口 NAT 可以配置 TCP 或 UDP 服务对象（object service 命令）。
- Twice NAT 支持路由模式和透明模式防火墙。
- 在透明模式中，必须指定真实和映射接口，不能使用 any。
- 在透明模式中，不能配置接口 PAT，因为透明模式接口没有 IP 地址。也不能将管理

IP 地址用于映射地址。

- 若欲修改 NAT 配置，并且在新的 NAT 信息应用前不想等待现有转换超时，可以使用 clear xlate 命令清除转换表。不过，清除转换表将断开所有当前正用于转换的连接。

> **提・示**　如果移除动态 NAT 或 PAT 规则，然后，再添加新的带有映射地址的规则，如果新规则中的地址与移除规则中的进行重叠，那么，在移除规则超时或使用 clear xlate 命令清除之前，所有连接新规则将不能被使用，以确保同一地址不被指定至多个主机。

- 用于 NAT 的对象和对象组必须是明确的，必须包括 IP 地址。
- 在多个规则中可以使用同一对象。
- 映射 IP 地址池不能包含：
  - 映射接口 IP 地址。如果为规则指定 any 接口，所有接口的 IP 地址都将不被接受。接口 PAT（只适用于路由模式）使用 interface 关键字代替 IP 地址。
  - （透明模式）管理 IP 地址。
  - （动态 NAT）启用 VPN 时，备用接口 IP 地址。
  - 现有 VPN 池地址。

2. 配置动态 NAT

为动态 NAT 配置 Twice NAT 操作过程如下。

① 配置真实源地址。可以配置为网络对象或网络对象组。如果想转换所有通信，可以跳过该步骤，并指定 any 关键字以代替创建对象或对象组。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

② 配置映射源地址。可以配置为网络对象或网络对象组。对于动态 NAT，通常配置大组地址用于映射小组。如果映射网络对象包含 IP 地址范围或主机 IP 地址，那么，IP 地址范围用于动态 NAT，主机 IP 地址用于 PAT 回退。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# range ip_address_1 ip_address_2
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | host
ip_address} | group-object grp_obj_name}
```

③（可选）配置真实目的地址。可以配置为网络对象或网络对象组。尽管实现 Twice NAT 的主要功能应当配置目的 IP 地址，但是，目的 IP 地址仍然不是必须要配置的。即使不指定目的地址，也可以配置静态转换，或者使用 Identity NAT。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address
netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name |
subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

④（可选）配置映射目的地址。目的转换通常是静态的。Identity NAT 可以跳过该步骤，真实和映射地址都可以简单地使用同一对象或组。如果想转换目的地址，可以配置网络对象或网络对象组。静态映射是典型的一对一，因此，真实地址与映射地址的数量相同。

对于带端口转换的静态接口 NAT（只适用于路由模式），可以跳过该步骤，并指定 interface 关键字代替映射地址的网络对象/组。

配置命令同上。

⑤（可选）为目的真实端口和目的映射配置服务对象。动态 NAT 不支持端口转换。不过，由于目的转换通常为静态，因此，可以在目的端口执行端口转换。服务对象可以包括源和目的端口，但是，只有目的端口能够使用。即使指定了源端口，也将被忽略。NAT 只支持 TCP 或 UDP。当转换一个端口时，确认真实和映射服务对象中的协议是相同的（两者或者都是 TCP，或者都是 UDP）。对于 Identity NAT，可以在真实和映射端口使用同一服务对象。不等于（neq）操作不被支持。

```
hostname(config)# object service obj_name
hostname(config-network-object)# service {tcp | udp} destination operator port
```

⑥ 配置动态 NAT。

```
hostname(config)# nat [(real_ifc,mapped_ifc)] [line | {after-auto [line]}]
source dynamic {real_obj | any} {mapped_obj [interface]} [destination static
{mapped_obj | interface} real_obj] [service mapped_dest_svc_obj real_dest_svc_obj]
[dns] [inactive] [description desc]
```

其中，

- 接口（Interface）（透明模式必需），指定真实和映射接口，确认在命令中使用了“()”。在路由模式中，如果不指定真实和映射接口，所有接口都将被使用。也可以为一个或两个接口指定关键字 any。
- 部分和行（可选），默认情况下，NAT 规则被添加至 NAT 表格第一部分的最后。如果想将规则添加到第 3 部分（即网络对象 NAT 规则之后），应当使用 after-auto 关键

字。也可以使用 line 将其插入规则中适当部分的任何位置。

- 源地址：
  - 真实地址，指定网络对象、组或 any 关键字（参见步骤 1）。如果想转换所有从真实接口至映射接口的通信，应当使用 any 关键字。
  - 映射地址，指定一个不同的网络对象或组（参见步骤 2）。
- 目的地址（可选）：
  - 映射地址，指定网络对象或组，或者带端口转换的静态接口 NAT，或者指定 interface 关键字（参见步骤 4）。如果指定了 interface，确认也配置了 service 关键字。对该选项必须为 real_ifc 配置指定接口。
  - 真实地址，指定网络对象或组（参见步骤 3）。对于 Identity NAT，真实和映射地址可以简单地使用同一对象或组。
- 目的端口（可选），与映射和真实服务对象同时指定 Service 关键字（参见步骤 5）。对于本体端口转换，简单地使用与真实和映射端口相同的服务对象即可。
- DNS（可选，只适用于源规则），DNS 关键字转换 DNS 应答。确认 DNS 检视被启用（默认为启用）。如果配置有 destination 地址，将不能再配置 DNS 关键字。
- Inactive（可选），将规则置于不可用状态，而不想移除该命令时，使用 inactive 关键字。若欲重新启用该规则，只需再次键入不包含 inactive 关键字的命令即可。
- 描述（可选），使用 description 关键字可以添加不超过 200 个字符的描述。

3. 配置动态 PAT（隐藏）

配置动态 PAT 的操作过程如下。有关关键字和参数说明，请参见上述相关内容，此处不复赘述。

① 配置真实源地址。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address
netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name |
subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

② 指定映射地址（即想转换为的地址）。可以配置一个单一地址，或者 PAT 池，或者多个地址。配置一个网络对象或对象组。网络对象组可以包含对象和/或内联地址。当然，如果想在 nat 命令中使用单一 IP 地址作为内联值，或者想借助 interface 关键字使用接口地址，也可以跳过该步骤。当映射地址用于 PAT 池，在对象或组中的所有地址，包含范围，被用于 PAT 地址。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | range ip_address_1
```

```
ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | host ip_address} | group-object grp_obj_name}
```

③ （可选）配置真实目的地址。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

④ （可选）配置映射目的地址。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

⑤ （可选）为目的真实端口和目的映射配置服务对象。

```
hostname(config)# object service obj_name
hostname(config-network-object)# service {tcp | udp} destination operator port
```

⑥ 配置动态 PAT（隐藏）。

```
hostname(config)# nat [(real_ifc,mapped_ifc)] [line | {after-auto [line]}] source dynamic {real-obj | any} {mapped_obj [interface] | [pat-pool mapped_obj [round-robin] [extended] [flat [include-reserve]] [interface] | interface} [destination static {mapped_obj | interface} real_obj] [service mapped_dest_svc_obj real_dest_svc_obj] [dns] [inactive] [description desc]
```

4. 配置静态 NAT 或带地址转换的静态 NAT

配置静态 NAT 或带地址转换的静态 NAT 的操作过程如下。有关关键字和参数说明，请参见上述相关内容，此处不复赘述。

① 步骤 1 至步骤 5 的操作过程与配置动态 PAT 相同。

② 配置静态 NAT。

```
hostname(config)# nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static real_ob [mapped_obj | interface] [destination static {mapped_obj | interface} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [dns] [no-proxy-arp] [inactive] [description desc]
```

5. 配置 Identity NAT

配置 Identity NAT 的操作过程如下。有关关键字和参数说明，请参见上述相关内容，此处不复赘述。

① 配置真实源地址。可以配置为网络对象或网络对象组。这些地址是欲执行 Identity NAT 的地址。若欲所有地址都执行 Identity NAT，可以跳过该步骤，并代之以关键字 any any。

网络对象：

```
hostname(config)# object network obj_name
hostname(config-network-object)# {host ip_address | subnet subnet_address netmask | range ip_address_1 ip_address_2}
```

网络对象组：

```
hostname(config)# object-group network grp_name
hostname(config-network-object)# {network-object {object net_obj_name | subnet_address netmask | host ip_address} | group-object grp_obj_name}
```

② （可选）配置真实目的地址。配置命令同上。

③ （可选）配置映射目的地址。配置命令同上。

④ （可选）为源或目的真实端口、源或目的映射端口配置服务对象。服务对象可以同时包含源和目的端口。不过，也可以为两个服务对象只指定源或目的端口。如果应用使用固定源端口（如 DNS 服务），可以同时指定源和目的端口，只是固定端口比较罕见而已。当转换端口时，确认真实和映射服务对象中使用的协议应当相同（两者均为 TCP 或 UDP）。对于 Identity NAT 而言，真实和映射端口可以使用同一服务对象。不等于（neq）操作不被支持。

```
hostname(config)# object service obj_name
hostname(config-network-object)# service {tcp | udp} [source operator port] [destination operator port]
```

⑤ 配置 Identity NAT。为真实和映射服务对象（参见步骤 4）指定 service 关键字。鉴于是源端口转换，对象必须指定为源服务。源端口转换命令中服务对象的排序，由 service real-obj mapped_obj 所决定。目的端口转换中的对象必须指定目的服务。目的端口转换命令中服务对象的排序，由 mapped_obj service real-obj 所决定。在对象中同时指定源和目的端口不常用到，首先服务对象包含真实源端口/映射目的端口，其次服务对象包含映射源端口/真实目的端口。对本体端口转换而言，真实和映射端口（源和/或目的端口，依配置而定）两者均需简单使用同一服务对象即可。

```
hostname(config)# nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}]source static {nw_obj nw_obj | any any} [destination static {mapped_obj | interface} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [no-proxy-arp] [route-lookup] [inactive] [description desc]
```

6. Twice NAT 配置示例

■ **依目的的转换（动态 PAT）**

位于 10.1.2.0/24 网络上的主机访问 2 台不同的服务器。当主机访问服务器 211.82.216.11 时，真实地址被转换为 211.82.220.29:port，当主机访问服务器 211.82.218.22 时，真实地址被转换为 211.82.220.30:port（如图 18-8 所示）。

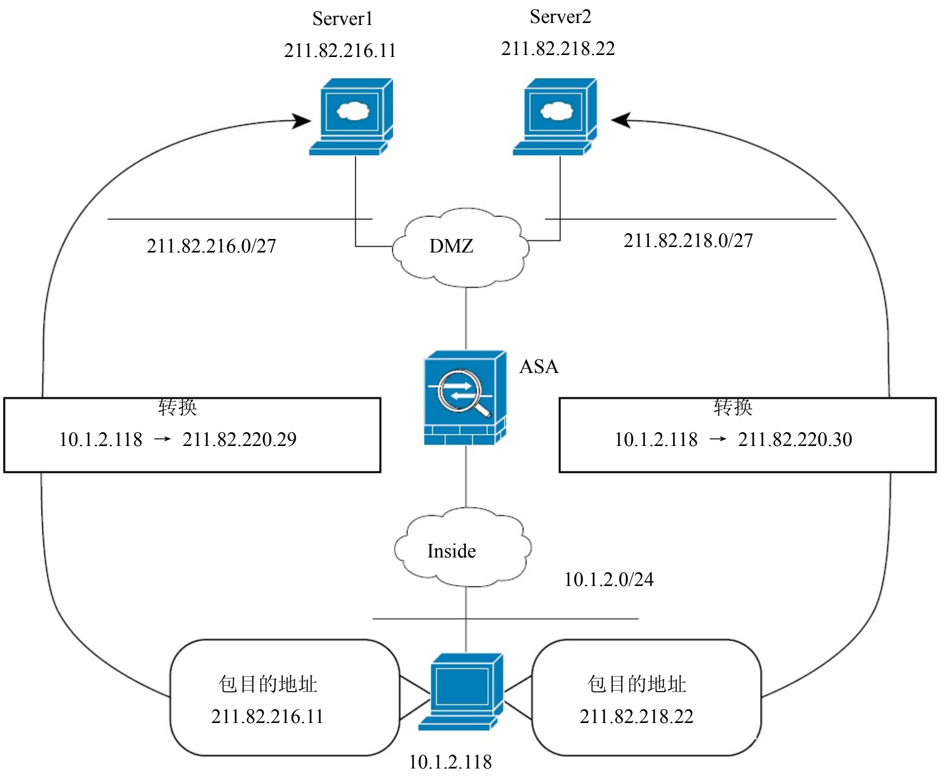


图 18-8 依目的的不同转换

配置过程如下：

① 为内部网络添加网络对象。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

② 为 DMZ 网络 1 添加网络对象。

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 211.82.216.0 255.255.255.224
```

③ 为 PAT 地址添加网络对象。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 211.82.220.29
```

④ 配置第 1 条 Twice NAT 规则。由于不想转换目的地址，因此，需要为真实和映射目的地址指定同一地址，以为配置 Twice NAT。默认情况下，NAT 规则被添加至 NAT 表的第一部

分末尾。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

⑤ 为 DMZ 网络 2 添加网络对象。

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 211.82.218.224 255.255.255.224
```

⑥ 为 PAT 地址添加网络对象。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 211.82.220.30
```

⑦ 配置第 2 条 Twice NAT 规则。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

■ **依目的地址和端口的转换（动态 PAT）**

10.1.2.0/24 网络上的主机访问位于一台主机上的 Web 服务器和 FTP 服务器。当主机访问 FTP 服务时，真实地址转换为 211.82.220.29:port，当主机访问同一服务器上的 Web 服务时，真实地址转换为 211.82.220.30:port（如图 18-9 所示）。

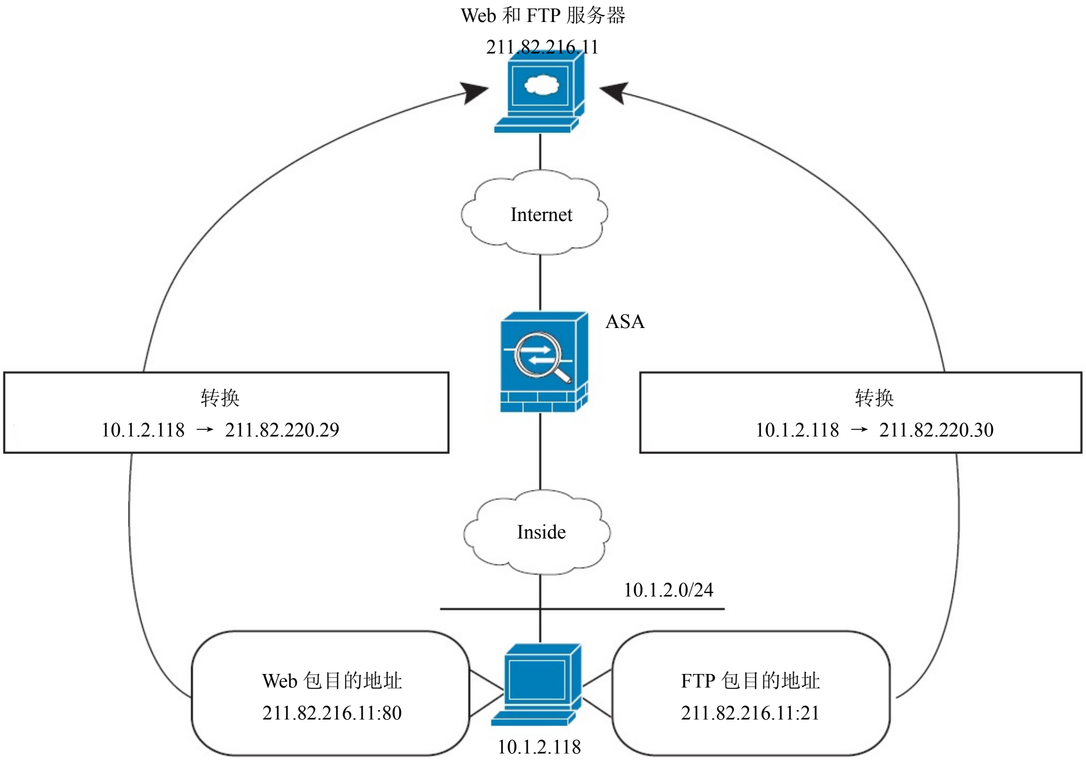


图 18-9　依目的地址和端口的转换（动态 PAT）

操作过程如下：

① 为内部网络添加网络对象。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

② 为 FTP/Web 服务器添加网络对象。

```
hostname(config)# object network FTPWebServer
hostname(config-network-object)# host 211.82.216.11
```

③ 为 PAT 地址添加使用 FTP 时的网络对象。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 211.82.220.29
```

④ 为 FTP 添加服务对象。

```
hostname(config)# object service FTPObj
hostname(config-network-object)# service tcp destination eq ftp
```

⑤ 配置第 1 条 Twice NAT 规则。由于不想转换目的地址或端口，因此，需要为真实和映射目的地址指定同一地址，以配置 Twice NAT。真实和映射服务使用同一端口。默认情况下，NAT 规则被添加至 NAT 表第 1 部分末尾。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1 destination static FTPWebServer FTPWebServer service FTPObj FTPObj
```

⑥ 为 PAT 地址添加使用 HTTP 时的网络对象。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 211.82.220.30
```

⑦ 为 HTTP 添加服务对象。

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

⑧ 配置第 2 条 Twice NAT 规则。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2 destination static FTPWebServer FTPWebServer service HTTPObj HTTPObj
```

18.7 配置访问控制

18.7.1 访问规则概述

可以通过将扩展或 EtherType 访问列表应用至某个接口或全局所有接口来创建访问规则，并借助这些访问规则来控制路由模式和透明防火墙模式下的 IP 通信。访问规则允许或拒绝基于协议的通信，包括源和目的 IP 地址或网络，以及源和目的端口。对于透明模式而言，EtherType

规则允许或拒绝基于 EtherType 的通信，即以非 IP 通信控制网络访问。

1. 访问规则

■ **隐示许可**

在路由模式下，默认允许从高安全接口至低安全接口的通信。

在透明模式下，默认允许从高安全接口至低安全接口的通信。ARP 和 BPDU 的双向通信。

对于其他通信而言，需要使用扩展访问规则，或者 EtherType 规则实现。

■ **接口访问规则和全局访问规则**

既可以应用访问规则至指定接口或全局所有接口，也可以在配置接口访问规则的同时配置全局访问规则，在这种情况下，指定接口访问规则将优先于全局访问规则执行。

> **提·示** 全局访问规则只应用于进站通信。

■ **在同一接口使用访问规则和 EtherType 规则**

可以应用一条访问规则和一条 EtherType 规则至接口的每个方向。

■ **隐示拒绝**

访问列表的末尾包含一个隐示拒绝，除非明示许可，通信不能通过。例如，想允许所有用户通过 ASA 访问除某个特定地址之外的网络，那么，需要拒绝该特定地址，并允许所有其他访问。

对于 EtherType 访问列表而言，位于访问列表末尾的隐示拒绝不会影响 IP 通信或 ARP。例如，如果允许 EtherType 8037，位于访问列表末尾的隐示拒绝不会阻塞任何事先借助扩展访问列表（或从高安全接口至低安全接口的隐示允许）允许的 IP 通信。然而，如果以 EtherType ACE 明示拒绝了所有通信，那么，IP 和 ARP 通信将被拒绝。

如果配置了全局访问规则，那么，隐示拒绝将被置于全局规则之后处理。操作顺序如下：

- 接口访问规则。
- 全局访问规则。
- 隐示拒绝。

■ **进站和出站规则**

ASA 支持两种类型的访问规则：

- 进站（Inbound）——进站访问规则应用至作为进入的接口。全局访问规则通常为进站。
- 出站（Outbound）——出站访问规则应用于作为外出的接口。

> **提·示** “Inbound” 和 “Outbound” 所指为在接口上应用访问列表，在接口上进入 ASA 的通信或在接口上外出 ASA 的通信。该术语不是指以下动作：从低安全接口至高安全接口的通信一般认为是进站，从高安全接口至低安全接口，一般认为是出站。

出站访问列表是可用的。例如，想只允许内部网络中的某个特定主机访问位于外部网络的 Web 服务器。与其创建多个入站访问列表以限制访问，不如创建一个出站访问列表只允许指定主机。外出访问列表阻止任何到达外部网络的其他主机（如图 18-10 所示）。

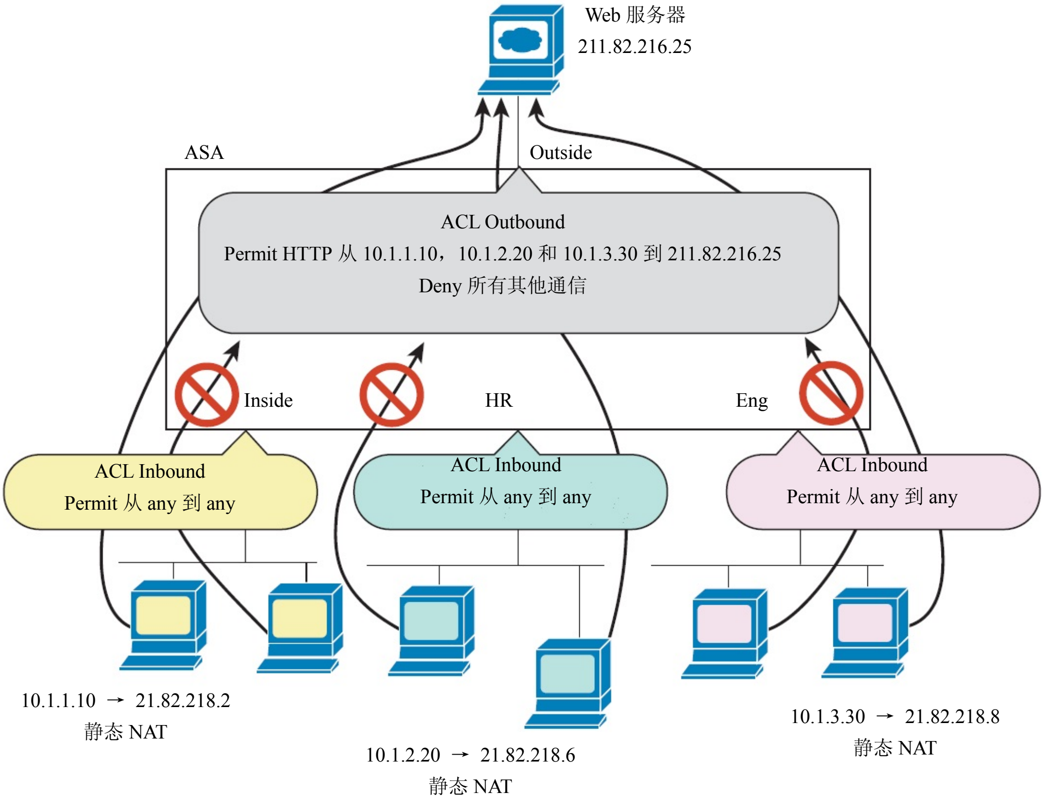


图 18-10　进站和出站规则示例

具体配置如下所示：

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.10 host 211.82.216.25 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.20 host 211.82.216.25 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.30 host 211.82.216.25 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

2. 扩展访问规则

■ **返回通信访问规则**

对于路由和透明模式下的 TCP 和 UDP 连接而言，无需访问规则允许返回通信，因为 ASA 允许所有已建立的、双向连接的通信。

对于无连接协议，如 ICMP，ASA 创建单向进程，访问规则需要在两个方向允许 ICMP（应用访问列表至源和目的接口），或者需要启用 ICMP 检视引擎。ICMP 检视引擎将 ICMP 进程作为双向连接处理。

■ **使用访问列表允许广播和多播通信通过透明防火墙**

在路由防火墙模式中，即使在访问规则中允许，广播和多播通信也将被阻塞，包括不被支持的动态路由协议和 DHCP（除非配置了 DHCP 中继）。透明防火墙模式能够允许任何 IP 通信通过。该功能在多环境模式中尤为重要。表 18-5 所示为能够通过透明模式防火墙的常见通信类型。

> **提·示** 由于这些特殊类型的通信是无连接的，因此，需要应用一个扩展访问列表至两个接口，从而保证返回通信能够通过。

表 18-5 透明防火墙特殊通信

通信类型	协议或端口	注 释
DHCP	UDP 端口 67 和 68	如果启用 DHCP 服务器，ASA 不能通过 DHCP 包
EIGRP	协议 88	-
OSPF	协议 89	-
多播流	依应用不同 UDP 端口也不同	多播流常常使用 D 类地址（224.0.0.0～239.0.0.0）
RIP（v1 或 v2）	UDP 端口 520	-

■ **管理访问规则**

能够配置访问规则控制管理发往 ASA 的通信。to-the-box 访问控制规则管理通信（由 http, ssh 或 telnet 等命令定义）较应用 control-plane 选项的管理访问规则有较高的优先级。因此，即使在 to-the-box 访问列表中明确拒绝，被许可的管理通信也将被允许进入。

3. EtherType 规则

■ **被支持的 EtherType 类型和其他通信**

EtherType 规则能够控制下列通信：

- EtherType 借助 16 位十六进制数字标识，包括常见的 IPX 和 MPLS 单播或多播。
- Ehternet V2 帧。
- BPDU，默认被许可。由于中继 BPDU 在有效荷载中带有 VLAN 信息，因此，如果允许 BPDU，那么，将为外出 VLAN 修改有效荷载。

- IS-IS，只在版本 8.4（5）支持。

> **提・示** 802.3 格式帧不被支持，因此这些帧没有规则的句柄。

■ **允许 MPLS**

若欲允许 MPLS，应当确保 LDP（Label Distribution Protocol，标签分发协议）和 TDP（Tag Distribution Protocol，标识分发协议）连接已经建立。

在 Cisco IOS 路由器上，可以输入下述命令：

```
hostname(config)# mpls ldp router-id interface force
```

或

```
hostname(config)# tag-switching tdp router-id interface force
```

18.7.2 配置和监视访问规则

1. 配置访问规则

将访问列表绑定至接口或全局。指定扩展、EtherType 访问列表名称。

可以为每端口每访问列表类型配置一个 access-group 命令。

不能引用空的访问列表或只有一条注释的访问列表。

接口指定规则：

in 关键字应用访问列表至入站通信。out 关键字应用访问列表至出站通信。

指定 interface 名称。

per-user-override 关键字（只用于入站访问列表）允许用户授权下载的动态用户访问列表覆盖指定至接口的访问列表。例如，如果接口访问列表拒绝所有来自 10.0.0.0 的通信，但是，动态访问列表允许所有来自 10.0.0.0 的通信，那么，动态访问列表将为用户覆盖接口访问列表。

control-plane 关键字指定规则适用于 to-the-box 通信。

对于全局规则而言，指定 global 关键字应用访问列表至入站方向的所有接口。

```
hostname(config)# access-group access_list {{in | out} interface interface_name
[per-user-override | control-plane] | global}
```

2. 监视访问规则

显示当前绑定至接口的访问规则。

```
show running-config access-group
```

3. 访问规则配置示例

access-liest 命令让任意主机使用 80 端口访问全局地址，access-group 命令指定 access-list

命令应用至外出接口的通信。

```
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

访问内部网络的 Web 服务器，其 IP 地址为 211.82.216.12。该 IP 地址为真实地址，NAT 之后的外部接口不能看到。

```
hostname(config)# access-list ACL_OUT extended permit tcp any host 211.82.216.12
eq www
hostname(config)# access-group ACL_OUT in interface outside
```

允许所有主机均在 inside 和 hr 两个网络之间通信，但是只有指定的主机（192.168.1.6 和 192.168.1.9）可以访问外部网络。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 192.168.1.6 any
hostname(config)# access-list OUT extended permit ip host 192.168.1.9 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

允许常见的 EtherType（如 IPX、MPLS 单播）在内部接口发起。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

允许一些 EthreType 通过 ASA。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

只拒绝 EtherType 0x1256 通信，允许其他所有两个接口之间的 EtherType 通信。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

使用对象组允许指定内部接口上的指定通信。

```
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog
interface inside any
```